**ATIS-0500032.v002**

ATIS Standard on -

# ATIS Standard for Implementation of an IMS-based NG9-1-1 Service Architecture

## Notice of Disclaimer & Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OFMERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to https://www.atis.org/policy/patent-assurances/ to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

*Published by*

**Alliance for Telecommunications Industry Solutions**
**1200 G Street, NW, Suite 500**
**Washington, DC 20005**

**ATIS-0500032.v002**

ATIS Standard on

# ATIS Standard for Implementation of an IMS-based NG9-1-1 Service Architecture

**Alliance for Telecommunications Industry Solutions**

Approved April 5, 2022

**Abstract**

This Standard defines the Stage 2 (architecture) and Stage 3 (protocol) specifications for an IMS-based NG9-1-1 Service Architecture. This Standard includes the architecture, functional elements, call flows, protocols, and interfaces which were derived from the Stage 1 requirements in ATIS-0500023, “Applying Common IMS to NG9-1-1 Networks”.

# Foreword

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers.

The ESIF IP Multimedia Subsystem for 9-1-1 (IMS911) subgroup led this joint work effort that addresses the application of common IMS (Stage 1, 2, and 3) for the processing, transport, and/or delivery of Emergency Service calls within the NG9-1-1 network to the appropriate Public Safety Answering Point (PSAP). This is a joint effort with the Emergency Services Interconnection Forum Next Generation Emergency Service (ESIF NGES) Subcommittee, Packet Technologies and Systems Committee (PTSC) and the Wireless Technologies and Systems Committee Systems and Network Subcommittee (WTSC SN).

The Emergency Services Interconnection Forum (ESIF) provides a forum to facilitate the identification and resolution of technical and/or operational issues related to the interconnection of wireline, wireless, cable, satellites, Internet and emergency services networks.

The ESIF Next Generation Emergency Services (NGES) Subcommittee coordinates emergency services needs and issues with and among SDOs and industry forums/committees, within and outside ATIS, and develops emergency services (such as E9-1-1) standards, and other documentation related to advanced (i.e., Next Generation) emergency services architectures, functions, and interfaces for communications networks.

The Packet Technologies and Systems Committees (PTSC) develops and recommends standards and technical reports related to services, architectures, and signaling, in addition to related subjects under consideration in other North American and international standards bodies. PTSC coordinates and develops standards and technical reports relevant to telecommunications networks in the U.S., reviews and prepares contributions on such matters for submission to U.S. ITU-T and U.S. ITU-R Study Groups or other standards organizations, and reviews for acceptability or per contra the positions of other countries in related standards developments and takes or recommends appropriate actions.

The Wireless Technologies and Systems Committee (WTSC) develops and recommends standards and technical reports related to wireless and/or mobile services and systems, including service descriptions and wireless technologies. WTSC develops and recommends positions on related subjects under consideration in other North American, regional, and international standards bodies.

The WTSC Systems and Networks Subcommittee (WTSC SN) develops, maintains, amends and enhances American National Standards and ATIS deliverables related to system aspects, networks, and terminals within the GSM family (GSM/EGPRS/UMTS) such as circuit-switched, packet-switched and IP Multimedia services including future developments.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, ESIF, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time of consensus on this document, the committees responsible for its development, had the following leadership:

D. Morkunas, ESIF Chair (Intrado)

J. Torres, ESIF First Vice-Chair (Verizon Wireless)

B. Abley, ESIF Second Vice-Chair (NENA)

T. Reese, ESIF IMS911 Co-Chair, ESIF NGES Co-Chair (Ericsson)

M. Dolly, PTSC Chair (AT&T)

V. Shaikh, PTSC Vice-Chair (Peraton Labs)

M. Younge, WTSC Chair (T-Mobile)

D. Zelmer, WTSC Vice-Chair (AT&T)

T. Brooks, WTSC SN Chair (T-Mobile)

P. Musgrove, WTSC SN Vice-Chair (AT&T)

# Table of Contents

# Table of Figures

# Table of Tables

ATIS Standard on –

# Implementation of an IMS-based NG9-1-1 Service Architecture

## Preface

ATIS has developed a Next Generation 9-1-1 network and emergency call processing architecture based on contributions received since 2011 and based on requirements by a number of wireless carriers to have an IP Multimedia Subsystem (IMS)-compatible NG9-1-1 design[1]. Additionally, the NENA i3 Architecture Working Group[2] deferred the IMS-based Emergency Services IP Network (ESInet) development to ATIS. ATIS' goal in developing this standard has been transparent interoperability between the two network designs.

ATIS' intent in this development work was to produce a standard method for IMS-based carriers to offer NG9-1-1 services wholly within their IMS platforms, while maintaining consistency and interoperability with the NENA i3 ESInet/NGCS (Next Generation Core Services) design goals. This kind of standards approach allows IMS-based carriers to take advantage of complete IMS interoperability and features found in their existing IMS ecosystems, while still remaining interoperable with downstream i3 PSAPs that implement NENA i3 standards and interfaces.

It is also ATIS' goal to assure that terminating NG9-1-1 entities, such as i3 PSAPs, find the upstream networks that are built on the ATIS IMS-based NG9-1-1 Service Architecture to be as completely interoperable with their systems and networks as that of a NENA i3 NG9-1-1 standard SIP-based architecture. This goal of transparency, both upstream and downstream between architectures, ensures that an i3 PSAP should find no difference whether the i3 PSAP interconnects to a NENA i3 ESInet with NGCS, or interconnects to an ATIS IMS-based NG9-1-1 Service Architecture. This consistent interoperability principle has guided all of ATIS' development work since the beginning, as documented within the original Issue Statement underlying this work.

The ATIS IMS-based NG9-1-1 Service Architecture provides compatibility for IMS-based carriers acting as an NG9-1-1 System Service Provider (911SSP) to seamlessly interoperate with NENA i3 ESInet architectures.

For entities early in the process of selecting ESInet solutions, the expectation within this ATIS development work was that the ATIS IMS-based NG9-1-1 Service Architecture would offer a choice for carriers that already had an IMS ecosystem, but not be considered a viable architecture choice for 9-1-1 service entities that had no plans for an IMS infrastructure.

Public Safety entities should naturally understand the applicability of an IMS-based NG9-1-1 Service Architecture network approach to processing emergency calls, yet in this case, they can remain confidently focused on NENA i3-based NG9-1-1 architectures, (this is because IMS may be of interest to carriers, not to jurisdictions), which means that Public Safety's progress and momentum to adopt NG9-1-1 will not be impeded by the introduction of this ATIS NG9-1-1 Service Architecture standard.

[1] IMS is a set of standards based on the IETF RFC 3261 [Ref 18] family of standards that also introduces additional requirements, specific for carrier operators not differentiated in the more general SIP RFCs.

[2] The NENA i3 Architecture Working Group developed NENA-STA-010.3 [Ref 27].

# 1 Scope, Purpose, & Application

## 1.1 Scope

This ATIS Standard applies IP Multimedia Subsystem (IMS) architecture concepts to Next Generation 9-1-1 (NG9-1-1) networks to encompass:

- Definition of an IMS-based NG9-1-1 Emergency Services Network architecture and set of additional gateway functional elements that are integrated into this IMS-based NG9-1-1 Service Architecture, adopted from the existing NENA i3 architecture, to support the delivery of emergency calls to legacy and NG9-1-1/i3 Public Safety Answering Points (PSAPs).
- NG9-1-1 network deployment scenarios showing an IMS-based NG9-1-1 Service Architecture interconnecting with a variety of originating network and PSAP types, and associated Stage 2/3 call flows.

## 1.2 Purpose

IMS standards for Emergency Services have been under development and enhancement in 3GPP since 3GPP Release 9. However, from a Next Generation Emergency Services (NG9-1-1) network perspective, the IMS architecture only defined Emergency Service call processing for the originating network and has not defined call processing, transport, or delivery of Emergency Service calls by an IMS-based NG9-1-1 Emergency Services Network.

The purpose of this Standard is to define the Stage 2 (architecture) and Stage 3 (protocols) to enable North American deployment of NG9-1-1 emergency services networks that are based upon the 3GPP IMS specifications. This IMS-based NG9-1-1 emergency services network is called IMS-based NG9-1-1 Service Architecture.

This Standard includes the architecture, functional elements, call flows, protocols, and interfaces which were derived from the Stage 1 requirements in ATIS-0500023, “Applying Common IMS to NG9-1-1 Networks” [Ref 26].

## 1.3 Application

The standard applies to requests for emergency services originating from legacy, IMS-based, and generic Voice over Internet Protocol (VoIP) originating networks by routing those emergency service requests to the appropriate PSAP. This standard applies to routing voice, text, and multimedia requests.

# 2 Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this ATIS Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this ATIS Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

[Ref 1] 3GPP TS 23.167, *Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS) emergency sessions*.[3]

[Ref 2] 3GPP TS 24.229, *Technical Specification Group Services and System Aspects; IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3*.[3]

[Ref 3] 3GPP TS 22.101, *Technical Specification Group Services and System Aspects; Service aspects; Service principles*.[3]

[Ref 4] 3GPP TS 23.002, *Technical Specification Group Services and System Aspects; Network architecture*.[3]

[3] This document is available from the Third Generation Partnership Project (3GPP) at: < http://www.3gpp.org/specs/specs.htm >.

[Ref 5] 3GPP TS 23.271, *Technical Specification Group Services and System Aspects; Functional Stage 2 description of Location Services (LCS)*.[3]

[Ref 6] IETF RFC 5222, *LoST: A Location-to-Service Translation Protocol*.[4]

[Ref 7] J-STD-036-C-2, *Enhanced Wireless 9-1-1 Phase II*.[5]

[Ref 8] IETF RFC 5139, *Revised Civic Location Format for Presence Information Data Format Location Object (PIDF-LO)*.[4]

[Ref 9] IETF RFC 6753, *A Location Dereferencing Protocol Using HELD*.[4]

[Ref 10] IETF RFC 5491, *GEOPRIV Presence Information Data Format Location Object (PIDF-LO) Usage Clarification, Considerations, and Recommendations*.[4]

[Ref 11] 3GPP TS 24.147, *Technical Specification Group Core Network and Terminals; Conferencing using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3*.[3]

[Ref 12] IETF RFC 7852, *Additional Data related to an Emergency Call*.[4]

[Ref 13] IETF 4353, *A Framework for Conferencing with the Session Initiation Protocol (SIP)*.[4]

[Ref 14] ATIS-1000679, *Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control or ISDN User Part*.[6]

[Ref 15] IETF RFC 6442, *Location Conveyance for the Session Initiation Protocol*.[4]

[Ref 16] IETF RFC 4119, *A Presence-based GEOPRIV Location Object Format*.[4]

[Ref 17] IETF RFC 3265, *Session Initiation Protocol (SIP) – Specific Event Notification*.[4]

[Ref 18] IETF RFC 3261, *SIP: Session Initiation Protocol*.[4]

[Ref 19] 3GPP TS 23.228, *Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS)*; Stage 2.[3]

[Ref 20] IETF RFC 4112, *Communications Resource Priority for the Session Initiation Protocol (SIP)*.[4]

[Ref 21] IETF RFC 7134, *The Management Policy of the Resource Priority Header (RPH) Registry* Changed to "IETF Review", March 2014.[4]

[Ref 22] IETF RFC 4579, *Session Initiation Protocol (SIP) Call Control - Conferencing for User Agents*[4]

[Ref 23] IETF RFC 7044, *An Extension to the Session Initiation Protocol (SIP) for Request History Information*.[4]

[Ref 24] IETF RFC 3455, *Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)*.[4]

[Ref 25] IETF RFC 3325, *Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks*.[4]

[Ref 26] ATIS-0500023, *Applying Common IMS to NG9-1-1 Networks*.[6]

[Ref 27] NENA-STA-010.3, *NENA i3 Standard for Next Generation 9-1-1*.[7]

[Ref 28] IETF RFC 7230, *Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing*.[4]

[Ref 29] IETF RFC 4103, *RTP Payload for Text Conversation*.[4]

[Ref 30] IETF RFC 4975, *The Message Session Relay Protocol (MSRP)*.[4]

[4] This document is available from the Internet Engineering Task Force (IETF) at: < http://www.ietf.org >.

[5] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS), 1200 G Street N.W., Suite 500, Washington, DC 20005 at: < https://www.atis.org/docstore/product.aspx?id=26080 >.

[6] This document is available from the ATIS, 1200 G Street N.W., Suite 500, Washington, DC 20005 at: < https://www.atis.org/docstore/product.aspx?id=25371 >.

[7] This document is available from the National Emergency Number Association at: < NENA Standards & Other Documents >

[Ref 31] IETF RFC 4575, *A Session Initiation Protocol (SIP) Event Package for Conference State*.[4]

[Ref 32] 3GPP TS 29.333, *Technical Specification Group Core Network and Terminals; Multimedia Resource Function Controller (MRFC) - Multimedia Resource Function Processor (MRFP) Mp interface: Procedures Descriptions*.[3]

[Ref 33] IETF RFC 7092, *A Taxonomy of Session Initiation Protocol (SIP) Back-to-Back User Agents*.[4]

[Ref 34] IETF RFC 7647, *Clarifications for the Use of REFER with RFC 6665*.[4]

[Ref 35] IETF RFC 3891, *The Session Initiation Protocol (SIP) "Replaces" Header*.[4]

[Ref 36] IETF RFC 8224, *Authenticated Identity Management in the Session Initiation Protocol (SIP)*.[4]

[Ref 37] IETF RFC 8225, *PASSporT: Personal Assertion Token*.[4]

[Ref 38] IETF RFC 8443, *Personal Assertion Token (PASSporT) Extension for Resource Priority Authorization*.[4]

[Ref 39] ATIS-1000074.v002, *Signature-based Handling of Asserted information using toKENs (SHAKEN)*.[5]

[Ref 40] ATIS-1000080.v004, *Signature-based Handling of Asserted information using toKENs (SHAKEN): Governance Model and Certificate Management*.[5]

[Ref 41] IETF RFC 7090, *Public Safety Answering Point (PSAP) Callback*.[4]

[Ref 42] IETF RFC 3326, *The Reason Header Field for the Session Initiation Protocol (SIP)*.[4]

[Ref 43] FIPS-PUB-140-2, *Security Requirements for Cryptographic Modules)*.[8]

[Ref 44] IETF RFC 9027, *Assertion Values for Resource Priority Header and SIP Priority Header Claims in Support of Emergency Services Networks*.[4]

[Ref 45] IETF RFC 3323, *A Privacy Mechanism for the Session Initiation Protocol (SIP)*.[4]

[Ref 46] IETF RFC 3325, *Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks*.[4]

[Ref 47] IETF RFC 7044, *An Extension to the Session Initiation Protocol (SIP) for Request History Information*.[4]

[Ref 48] IETF RFC 8588, *Personal Assertion Token (PaSSporT) Extension for Signature-based Handling of Asserted information using toKENs (SHAKEN)*[4]

[Ref 49] 3GPP TS 24.629, *3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Explicit Communication Transfer (ECT) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification*.[3]

[Ref 50] IETF RFC 3515, *The Session Initiation Protocol (SIP) Refer Method*.[4]

[Ref 51] NENA-INF-011.2-2020, *NENA NG9-1-1 Policy Routing Rules Operations Guide*.[7]

[Ref 52] IETF RFC 8141, *Uniform Resource Names (URNs)*.[4]

[Ref 53] IETF RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.[4]

[Ref 54] OGC 10-069r2, *OWS 7 Engineering Report – Geosynchronization service*.[11]

[Ref 55] IETF RFC 4287, *The Atom Syndication Format*.[4]

[Ref 56] IETF RFC 5023, *The ATOM Publishing Protocol*.[4]

[Ref 57] ATIS-1000098, *Session Initiation Protocol (SIP) Resource-Priority Header (RPH) and Priority Header Signing in Support of Emergency Calling*.[5]

[Ref 58] NENA 75-001, *Security for Next Generation 9-1-1 Standard (NG-SEC)*.[8]

[Ref 59] NENA-INF-040.2, *NENA Monitoring and Managing NG9-1-1 Information Document*. (to be issued) [7]

[8] This document is available from the National Institute of Standards and Technology (NIST) at: < https://www.nist.gov/ >.

[Ref 60] IETF draft-ietf-ecrit-lost-planned-changes, *Validation of Locations Around a Planned Change*.[4]

[Ref 61] IETF RFC 6772, *Geolocation Policy: A Document Format for Expressing Privacy Preferences for Location Information*.[4]

[Ref 62] IETF RFC 7866, *Session Recording Protocol*.[4]

[Ref 63] NENA-STA-08-001, *NENA Interim VoIP Architecture for Enhanced 9-1-1 Services (i2)*.[7]

[Ref 64] NENA-STA-006.1-2018, *NENA Standard for NG9-1-1 GIS Data Model*.[7]

# 3 Informative References

The following standards contain provisions which, through reference in this text, constitute provisions of this ATIS Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this ATIS Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

[Ref 101] NENA-ADM-000.24-2021, *NENA Master Glossary of 9-1-1 Terminology*.[9]

# 4 Definitions, Acronyms, & Abbreviations

## 4.1 Definitions

| | |
|---|---|
| E.164 Number | E.164 is an international numbering plan for public telephone systems in which each assigned number contains a country code (CC), a national destination code (NDC), and a subscriber number (SN). There can be up to 15 digits in an E.164 number. The E.164 plan was originally developed by the International Telecommunication Union (ITU). |
| Emergency Call Routing Function (ECRF)[10] | A functional element in NGCS (Next Generation Core Services) which is a LoST protocol server where location information (either civic address or geo-coordinates) and a Service URN serve as input to a mapping function that returns a URI used to route an emergency call toward the appropriate PSAP for the caller's location or towards a responder agency.[10] |
| Emergency Services IP Network (ESInet)[9] | A managed IP network that is used for emergency services communications, and which can be shared by all public safety agencies. It provides the IP transport infrastructure upon which independent application platforms and core services can be deployed, including, but not restricted to, those necessary for providing NG9-1-1 services. ESInets may be constructed from a mix of dedicated and shared facilities. ESInets may be interconnected at local, regional, state, federal, national, and international levels to form an IP-based inter-network (network of networks). The term ESInet designates the network, not the services that ride on the network. |
| IMS-based NG9-1-1 Service Architecture | An IMS-based NG9-1-1 Service Architecture provides transit, routing, and other services required to support citizen-to-authority multimedia emergency services between the originating network and the emergency authority, e.g., PSAP. The IMS-based NG9-1-1 Service Architecture includes the i3 Legacy Network Gateway and i3 Legacy PSAP Gateway. |

[9] Available from the National Emergency Number Administration (NENA) at: < NENA Master Glossary >.

[10] Refer to NENA-ADM-000.24-2021, NENA Master Glossary of 9-1-1 Terminology [Ref 101].

| | |
|---|---|
| Legacy Network Gateway (LNG) | A signaling and media interconnection point between callers in legacy wireline/wireless originating networks and the IMS-based NG9-1-1 Emergency Services Network. This Functional Element provides Multi Frequency (MF)/Signaling System Number 7 (SS7)-to-SIP signaling interworking, as well as emergency services-specific processing of legacy emergency originations and location acquisition/dereferencing functionality. |
| Legacy PSAP Gateway (LPG) | A signaling and media interconnection point between the IMS-based NG9-1-1 Emergency Services Network and legacy PSAPs. This Functional Element provides SIP-to-Traditional/Enhanced MF signaling interworking as well as emergency services-specific processing to support: the delivery of emergency originations to legacy PSAPs; emergency call transfers involving legacy PSAPs; ALI queries from legacy PSAPs; and location and additional data dereferencing functionality. |
| Location by Reference (LbyR) | Location by Reference refers to the option to deliver a location reference URI in a header of the call request (SIP INVITE) that may be used by the requesting entity (e.g., the PSAP) to query for the location of the caller. |
| Location by Value (LbyV) | Location by Value refers to the option to deliver the caller's location to the PSAP within the body of the call request (SIP INVITE). |
| NG9-1-1[11] | An IP-based system comprised of hardware, software, data, and operational policies and procedures that: (A) provides standardized interfaces from emergency call and message services to support emergency communications; (B) processes all types of emergency calls, including voice, data, and multimedia information; (C) acquires and integrates additional emergency call data useful to call routing and handling; (D) delivers the emergency calls, messages, and data to the appropriate public safety answering point and other appropriate emergency entities; (E) supports data or video communications needs for coordinated incident response and management; and (F) provides broadband service to public safety answering points or other first responder entities.[9] |
| Non Call Associated Signaling (NCAS) | NCAS is a signaling method for legacy wireless calls where the calling (E.164) number and the Reference Identifier are sent. The Reference Identifier is used for routing calls. Both the calling number and the Reference Identifier may be used for retrieving location and additional data.<br>(a) If the call is delivered over an SS7 trunk group, the call setup signaling includes the calling number sent in the Calling Party Number parameter, the Reference Identifier is sent in the SS7 Generic Digits Parameter (GDP), and the digits "911" in the SS7 Called Party Number parameter.<br>(b) If the call is delivered over an MF trunk group, the call setup signaling includes the Reference Identifier signaled as the called number, and the calling number signaled as the Automatic Number Identification (ANI). |
| pANI (Pseudo Automatic Number Identification) | A telephone number used to support routing of wireless 9-1-1 calls. It may identify a wireless cell, cell sector, or PSAP to which the call should be routed. Also known as routing number. |
| Policy Store | A functional element in the ESInet that stores policy documents. |

[11] The term "NG911" used throughout this document is synonymous with the term "NG9-1-1".

| | |
|---|---|
| Reference Identifier | The term "Reference Identifier" is used in this standard to associate the call with location information of the caller. For routing to a legacy emergency services network, a Reference Identifier may be an Emergency Services Routing Key (ESRK) or Emergency Services Routing Digit (ESRD) as defined in J-STD-036-C-2 [Ref 7]. It may be the Telephone Number that is used by the legacy emergency services network to query for location information. In a legacy emergency services network, the Reference Identifier may also be used by the emergency services network to route the call to the PSAP. For calls routed to a NENA i3 ESInet, the Reference Identifier may be a dereferencing URI that is used by i3 functional elements and i3 PSAPs to obtain location.[12] |
| SHAKEN (Signature-based Handling of Asserted Information Using toKENs) | An industry framework for managing the deployment of Secure Telephone Identity (STI) technologies with the purpose of providing end-to-end cryptographic authentication and verification of the telephone identity and other information in an Internet Protocol (IP)-based service provider voice network. |
| Wireline Compatibility Mode (WCM) | WCM is a signaling method for legacy wireless calls where only the Reference Identifier is sent and used for routing, and for retrieving location and additional data. The originating Mobile Switching Center (MSC) sends an emergency call origination from a legacy wireless caller to the Legacy Network Gateway over an MF or SS7-supported trunk group. The call setup signaling includes the Reference Identifier (as the calling number) and the digits “911” (as the called number). |

## 4.2 Acronyms & Abbreviations

| | |
|---|---|
| 3GPP | Third Generation Partnership Project |
| ACM | SS7 Address Complete Message |
| ADR | Additional Data Repository |
| AES | Advanced Encryption Standard |
| ALI | Automatic Location Identification |
| ANI | Automatic Number Identification |
| ANM | SS7 Answer Message |
| AS | Application Server |
| ATIS | Alliance for Telecommunications Industry Solutions |
| B2BUA | Back-to-Back User Agent |
| BGCF | Breakout Gateway Control Function |
| CAMA | Centralized Automatic Message Accounting |
| cid | Content-ID |
| CdPN | Called Party Number |
| CPN | Calling Party Number |
| CSeq | Command Sequence |
| CVT | Call Validation Treatment |
| DDoS | Distributed Denial of Service |
| DHCP | Dynamic Host Configuration Protocol |

[12] Use of an Emergency Services Query Key (ESQK) as a Reference Identifier is for further study, pending the definition of use cases and call flows that illustrate the circumstances under which an ESQK applies.

| | |
|---|---|
| DNS | Domain Name System |
| DoS | Denial of Service |
| DR | Discrepancy Report |
| DTMF | Dual Tone Multi-Frequency |
| E-CSCF | Emergency Call Session Control Function |
| ECRF | Emergency Call Routing Function (NENA i3) |
| EIDO | Emergency Incident Data Object |
| E-MF | Enhanced MF |
| ESInet | Emergency Services IP Network |
| ESN | Electronic Serial Number or Emergency Service Number |
| ESQK | Emergency Services Query Key |
| ESRD | Emergency Services Routing Digits |
| ESRK | Emergency Services Routing Key |
| FG | Feature Group |
| FQDN | Fully Qualified Domain Name |
| GDP | Generic Digits Parameter |
| GIS | Geographic Information System |
| GMLC | Gateway Mobile Location Center |
| HELD | HTTP-Enabled Location Delivery |
| HTTP | Hypertext Transfer Protocol |
| HTTPS | HTTP Secure |
| IBCF | Interconnection Border Control Function |
| I-CSCF | Interrogating Call Session Control Function |
| IMEI | International Mobile Equipment Identity |
| IMS | IP Multimedia Subsystem |
| IP | Internet Protocol |
| ISDN | Integrated Services Digital Network |
| ISUP | ISDN User Part |
| JSON | JavaScript Object Notation |
| JWS | JSON Web Signature |
| KP | Key Pulse |
| LbyR | Location by Reference |
| LbyV | Location by Value |
| LIS | Location Information Server |
| LNG | Legacy Network Gateway |
| LoST | Location-to-Service Translation (protocol) |
| LPG | Legacy PSAP Gateway |
| LRF | Location Retrieval Function |
| LS | Location Server |
| LVF | Location Validation Function |
| MF | Multi Frequency |
| MGCF | Media Gateway Control Function |
| MGW | Media Gateway |
| MPC | Mobile Positioning Center |

| | |
|---|---|
| MRFC | Media Resource Function Controller |
| MRFP | Media Resource Function Processor |
| MSAG | Master Street Address Guide |
| MSC | Mobile Switching Center |
| NANP | North American Numbering Plan |
| NCAS | Non Call Associated Signaling |
| NENA | National Emergency Number Association |
| NG9-1-1 | Next Generation 9-1-1 |
| NNI | Network-to-Network Interface |
| NPD | Numbering Plan Digit |
| OGC | Open Geospatial Consortium |
| OLI (oli) | Originating Line Information (parameter) |
| OSP | Originating Service Provider |
| PAI | P-Asserted-Identity |
| PCA | PSAP Credentialing Agency |
| PIDF-LO | Presence Information Data Format – Location Object |
| PRF | Policy Routing Function |
| PSAP | Public Safety Answering Point |
| RLC | SS7 Release Complete |
| RDF | Routing Determination Function |
| REL | SS7 Release Message |
| RPH | Resource-Priority Header |
| RTT | Real Time Text |
| SBC | Session Border Controller |
| S-CSCF | Serving Call Session Control Function |
| SDP | Session Description Protocol |
| SHAKEN | Signature-based Handling of Asserted information using toKENs |
| SI | Spatial Interface |
| SIP | Session Initiation Protocol |
| SKS | Secure Key Store |
| SS7 | Signaling System Number 7 |
| STI | Secure Telephone Identity |
| STI-AS | Secure Telephone Identity Authentication Service |
| STI-CA | Secure Telephone Identity Certification Authority |
| STI-CR | Secure Telephone Identity Certificate Repository |
| STI-VS | Secure Telephone Identity Verification Service |
| TDM | Time Division Multiplexing |
| TLS | Transport Layer Security |
| TN | Telephone Number |
| TRF | Transit Function |
| TrGW | Transition Gateway |
| UDP | User Datagram Protocol |
| URI | Uniform Resource Identifier |
| URL | Uniform Resource Locator |

| | |
|---|---|
| URN | Uniform Resource Name |
| VoIP | Voice over IP |
| VSP | VoIP Service Provider |
| WCM | Wireline Compatibility Mode |
| WFS | Web Feature Service |

# 5 Introduction

The emergency services landscape within North America provides a greater level of detail than has been specified by 3GPP. Specifically, 3GPP only defined emergency procedures in originating networks and did not explicitly develop requirements for emergency services networks.

This standard provides additional details to the 3GPP IMS specifications to support the application of IMS in emergency services networks within North America. It addresses interconnection from originating legacy, IP-based IMS, and IP-based non-IMS networks. It also addresses emergency call delivery to both i3 and legacy PSAPs. This standard uses 3GPP IMS standards as its base and consideration must be given to how the specific aspects of the 3GPP IMS standards apply within the context of the North American emergency services architecture.

North American origination networks originate emergency calls (which include steps taken by originating device and network elements) and route such calls to a terminating IMS-based NG9-1-1 Emergency Services Network as defined in this standard.

This standard supports all classes of service and media types, and is not limited to voice.

# 6 Assumptions & Requirements

## *6.1 Basic Assumptions*

Assumptions used to develop this standard are based on those defined in the Stage 1 document ATIS-0500023 [Ref 26] and are modified to reflect the evolution of the IMS-based NG9-1-1 Service Architecture.

1. Calls may ingress from legacy originating networks and require no changes to those networks.
2. Based upon routing criteria, calls ingressing from legacy originating networks or from Originating Service Provider (OSP) networks that use NENA i3 compliant interfaces will be delivered either to legacy PSAPs or NENA i3 compliant PSAPs.
3. Calls ingressing from OSP networks that use NENA i3 compliant interfaces may include Location-by-Value (LbyV) or Location-by-Reference (LbyR).
4. If calls are received with LbyR, the IMS-based NG9-1-1 Service Architecture network will have to de-reference the location reference to retrieve the LbyV in order to route the call.
5. The IMS-based NG9-1-1 Service Architecture must support sending, receiving, and transfer of calls from/to NENA i3 compliant ESInets and from/to legacy emergency services networks. (Details related to the interconnection of the IMS-based NG9-1-1 Service Architecture with other legacy and Next Generation Emergency Services Networks are outside the scope of this Standard.) The IMS-based NG9-1-1 Service Architecture will route calls based upon location with or without policy considerations. Note that the location may be received (by value) with the call or the IMS-based NG9-1-1 Service Architecture may have to retrieve location.
6. Calls delivered to legacy PSAPs will include either the calling number/ANI or a pANI, and in some cases a callback number. The legacy PSAP will have to query the LPG to retrieve the location and, if not previously received, the callback number.

7. For calls from fixed or nomadic VoIP or IMS OSP networks, the IMS-based NG9-1-1 Service Architecture should deliver LbyV to the NENA i3 compliant PSAP.
8. For calls from mobile OSP networks, the IMS-based NG9-1-1 Service Architecture should deliver LbyR to the NENA i3 compliant PSAP. The NENA i3 PSAP must be able to de-reference the LbyR to retrieve a LbyV. The de-reference request may follow different paths depending on where the LbyR was generated.
    a. If the LbyR received by the i3 PSAP was generated by an LRF in an IMS-based originating network, the i3 PSAP will query the LRF in the originating network to retrieve the LbyV.
    b. If the LbyR received by the i3 PSAP was generated by a Location Information Server (LIS)/Location Server (LS) in a VoIP access network, the i3 PSAP will query the LIS/LS in the VoIP access network to retrieve the LbyV.
    c. If the originating network is a legacy wireless network, then gateway functionality within the LNG will be responsible for generating the LbyR that is delivered to the i3 PSAP. In this scenario, the i3 PSAP will query the LNG, and that element will be responsible for interacting with a Mobile Positioning Center (MPC)/Gateway Mobile Location Center (GMLC) in the legacy wireless originating network.
9. For the purposes of this document, VoIP fixed, nomadic, and mobile emergency services have all been addressed by Originating Service Providers.
10. The IMS-based NG9-1-1 Emergency Services Network described in this specification will replicate the functionality provided by a NENA i3 ESInet and associated functional elements. Any differences in the way that functionality is distributed among the elements of the IMS-based NG9-1-1 Emergency Services Network when compared to the NENA i3 NG9-1-1 architecture will be transparent to the PSAPs and originating networks served by the IMS-based NG9-1-1 Emergency Services Network.
11. Direct interconnection of interim VoIP originating networks to IMS-based NG9-1-1 Emergency Services Networks is left to implementation. Support for emergency originations from interim VoIP networks that are routed via a legacy Selective Router (as described in NENA 08-001 [Ref 63], Version 2) to an IMS-based NG9-1-1 Emergency Services Networks will be addressed as part of a future work item.
12. If an IMS-based NG9-1-1 Emergency Services Network applies caller identity and/or Resource-Priority Header (RPH) verification associated with a 9-1-1 call, as described in Clauses 7.3.1, 7.4, 8.12.1 and 8.12.2, the IMS-based NG9-1-1 Emergency Services Network will include the Identity headers and the results of the verification process in the SIP INVITE message forwarded to the i3 PSAP or Legacy PSAP Gateway.

## *6.2 Requirements*

Requirements used to develop this standard are defined in the Stage 1 document ATIS-0500023 [Ref 26]. See Clauses 7.3 and 9 for requirements in support of Secure Telephone Identity (STI) Services.

# 7 Architecture

## *7.1 Overview*

Figure 7-1 contains an illustration of the IMS origination network emergency call architecture from 3GPP TS 23.167 [Ref 1].

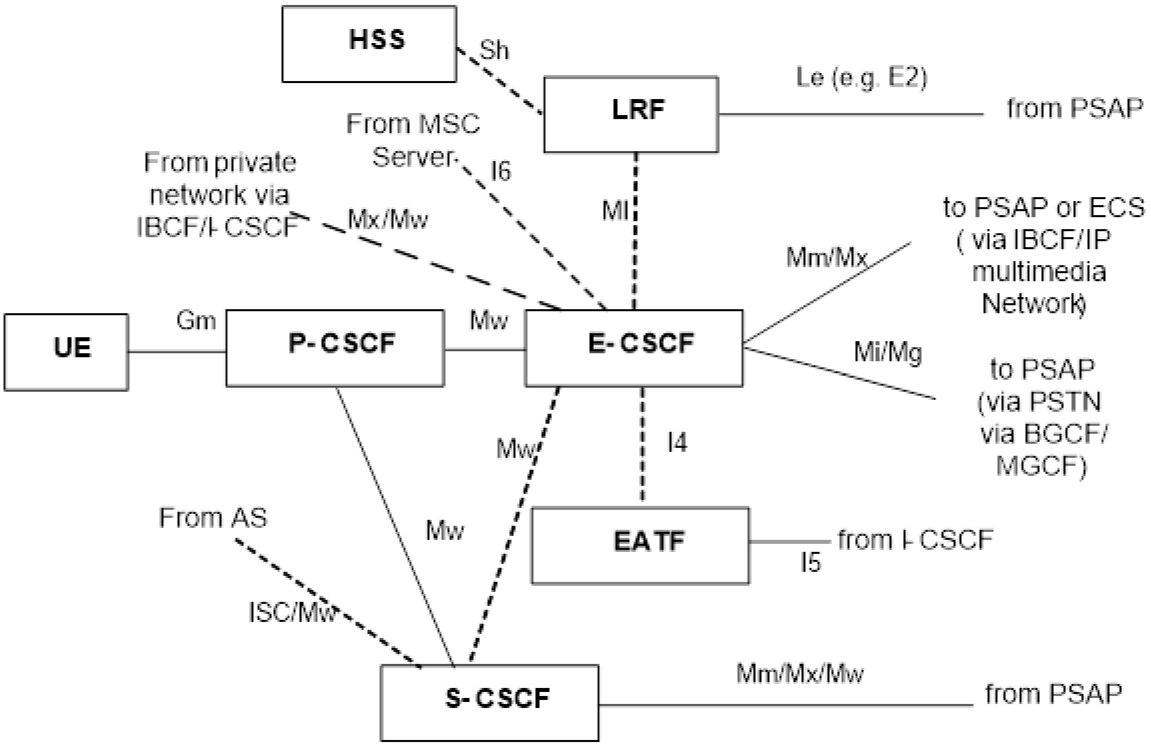


**Figure 7.1: IMS origination network emergency call architecture from 3GPP TS 23.167**

For a more complete architectural view, see 3GPP TS 23.002 [Ref 4].

Figure 7-2 illustrates an expanded architecture.

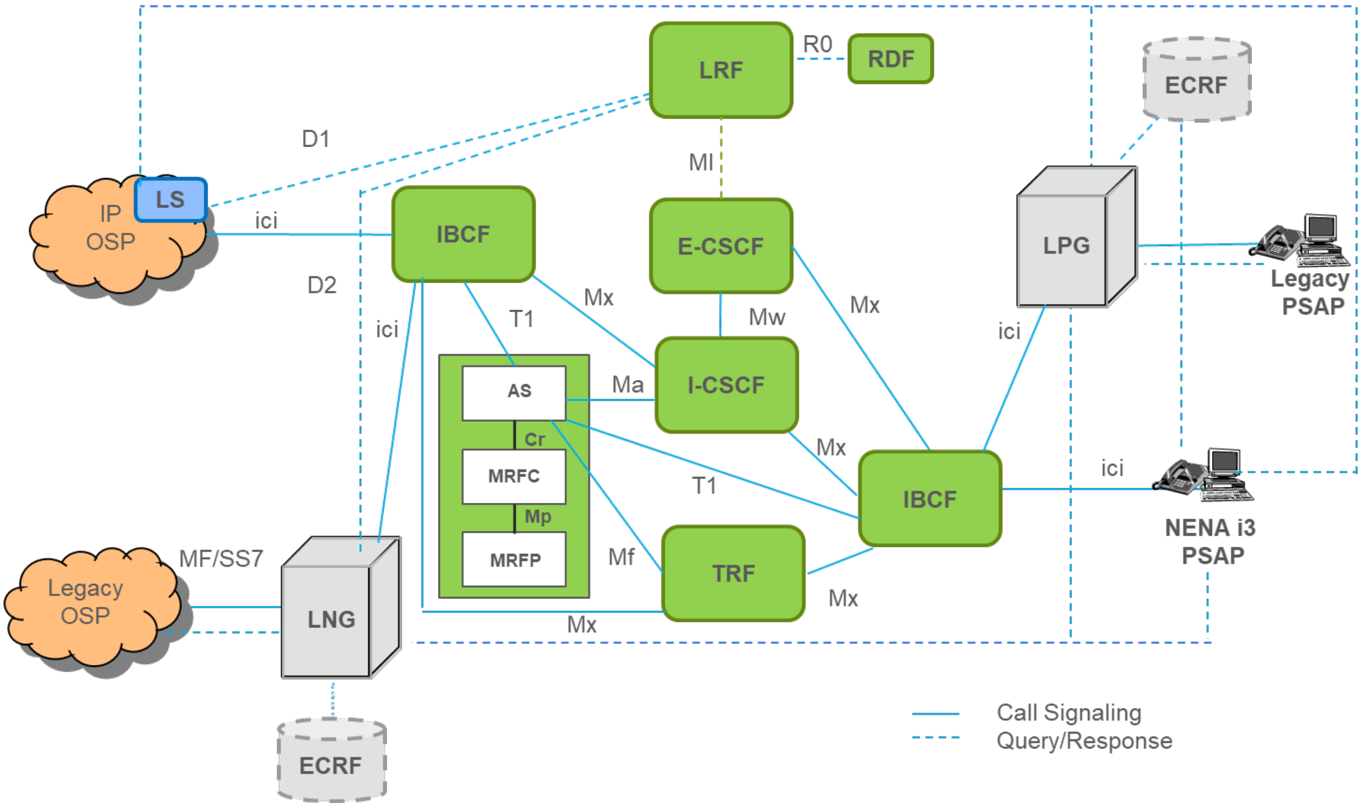


Figure 7.2: IMS-Based NG9-1-1 Service Architecture

## *7.2 IMS-Based NG9-1-1 Service Architecture Functional Elements*

This clause introduces the functional elements defined within this standard. Specific 3GPP standards are referenced for the applicable functional elements recognizing that the 3GPP standards refer to the operation of the functional elements in an IMS-based originating network. This standard refines the use of these IMS functional elements for applicability within an IMS-based NG9-1-1 Emergency Services Network. Where applicable, NENA i3 standards are referenced for detailed descriptions of the i3 functional elements that have been incorporated into the IMS-based NG9-1-1 Service Architecture described in this standard.

### 7.2.1 Emergency Call Session Control Function (E-CSCF)

The Emergency Call Session Control Function is used here as defined in 3GPP TS 23.167 [Ref 1] and its applicability is extended in this standard.

The E-CSCF receives the emergency session establishment request from the Interrogating Call Session Control Function (I-CSCF), queries the LRF for routing information, and forwards the call request toward the appropriate PSAP per the routing information. After initial call routing to the appropriate PSAP, the E-CSCF may or may not remain in the call path per implementation.

### 7.2.2 Interrogating Call Session Control Function (I-CSCF)

The Interrogating Call Session Control Function is used here as defined in 3GPP TS 23.228 [Ref 19] and its applicability is extended in this standard.

### 7.2.3 Location Retrieval Function (LRF)

The Location Retrieval Function (LRF) is used here as defined in 3GPP TS 23.167 [Ref 1] and its applicability is extended within this standard.

The LRF is queried by the E-CSCF and may obtain location information from the LS in the IP Originating Service Provider Network or from the LNG, if it is not provided in the call request (i.e., the location information is provided by reference and not by value). Either the location obtained from the LS/LNG or the location included in the emergency call request (i.e., LbyV) is used to query the RDF. The LRF obtains routing information for an emergency session from the Routing Determination Function (RDF). It returns the routing information to the E-CSCF.

### 7.2.4 Routing Determination Function (RDF)

The Routing Determination Function (RDF) is used here as defined in 3GPP TS 23.167 [Ref 1] and its applicability is expanded within this standard.

The RDF provides routing information for an emergency session based upon the location information in a request from the LRF. This routing information will designate a legacy PSAP or a NENA i3 PSAP.

### 7.2.5 Location Server (LS)

The Location Server (LS) is used here as defined in 3GPP TS 23.167 [Ref 1] and its applicability is extended in this standard. 3GPP 23.271 [Ref 5] allows the LS to be incorporated within the LRF. For this standard the LS resides within the Originating Service Provider network. If the emergency call request does not have the location information (by-value) contained within it, the LRF or LPG or i3 PSAP may query (i.e., send a dereference request to) the LS in the IP Originating Service Provider network to obtain it. If the IP Originating Service Provider network is a non-IMS i3-compliant originating network, the LS represents a LIS.  If the IP Originating Service Provider network is an IMS-based network, the LS will be queried via an LRF in the Originating Service Provider network. The LS functionality is dependent upon the type of call in order to obtain location information and is out of scope of this Standard.

### 7.2.6 Interconnection Border Control Function (IBCF)

The Interconnection Border Control Function (IBCF) is used here as defined in 3GPP TS 23.228 [Ref 19] and in 3GPP TS 23.167 [Ref 1] and its applicability is expanded in this standard. In this standard, with respect to emergency (9-1-1) originations, the IBCF functions on the ingress side of the IMS-based NG9-1-1 Emergency Services Network for calls originated from legacy and IP-based originating networks and on the egress side of the IMS-based NG9-1-1 Emergency Services Network when terminating calls to legacy PSAPs and NENA i3 PSAPs. With respect to callback calls, the ingress IBCF is the PSAP-facing IBCF, and the egress IBCF faces a directly interconnected originating network (i.e., the network from which the original emergency call originated) or a transit network. In the IMS-based NG9-1-1 Service Architecture, the IBCF will play the role of both the entry point into an IMS-based NG9-1-1 Emergency Services Network and the exit point from an IMS-based NG9-1-1 Emergency Services Network.

#### 7.2.6.1 Entry Point IBCF

In the context of emergency (9-1-1) originations, an entry point IBCF in an IMS-based NG9-1-1 Emergency Services Network will receive emergency call requests from an originating network and will forward them to an I-CSCF in the IMS-based NG9-1-1 Emergency Services Network for further processing. In the context of callback calls, an entry point IBCF in an IMS-based NG9-1-1 Emergency Services Network will receive callback calls from PSAPs and forward them to a Transit Function within the IMS-based NG9-1-1 Emergency Services Network. See Clause 9.6.1 for details related to the processing performed by an entry point IBCF.

#### 7.2.6.2 Exit Point IBCF

In the context of emergency (9-1-1) originations, an exit point IBCF in an IMS-based NG9-1-1 Emergency Services Network will receive emergency calls from an E-CSCF in an IMS-based NG9-1-1 Emergency Services Network and forward them to a PSAP for further processing. In the context of callback calls, an exit point IBCF will receive callback calls from the Transit Function within an IMS-based NG9-1-1 Emergency Services Network and forward them to an interconnecting IP network. See Clause 9.6.2 for details related to the processing performed by an exit point IBCF.

### 7.2.7 Legacy Network Gateway (LNG)

The LNG is a signaling and media interconnection point between callers in legacy wireline/wireless originating networks and the IMS-based NG9-1-1 Emergency Services Network. The LNG is responsible for interworking the Signaling System Number 7 (SS7) or Multi Frequency (MF) signaling that it receives from the legacy originating network to the SIP signaling used in the IMS-based NG9-1-1 Emergency Services Network. The LNG will use standard SS7-SIP interworking, as defined in ATIS-1000679 [Ref 14]. To support emergency call routing, the LNG applies service-specific interworking functionality to legacy emergency calls to allow the information provided in the call setup signaling by the wireline switch or MSC (e.g., calling number/ANI, ESRK, cell site/sector represented by an ESRD) to be used as input to the retrieval of location information (i.e., routing location) from an associated location server/database. The LNG uses the location information to query an ECRF to obtain routing information in the form of a URI. Based on implementation, the ECRF could be an RDF. The LNG then forwards the call/session request to an I-CSCF in the IMS-based NG9-1-1 Emergency Services Network, using the URI provided by the ECRF, and includes callback and location information (either by-value or by-reference) in the outgoing signaling. The LNG also supports interfaces to MPCs/GMLCs in legacy wireless originating networks to support the acquisition of caller location. To facilitate the use of LbyR, the LNG must support a dereference interface so that it can process dereference requests from other Functional Elements or PSAPs. In addition, the LNG may generate a data structure that contains additional non-location data associated with the call (e.g., class of service, provider contact information). The LNG may include the Additional Data (or a subset of it) “by-value” in the body of the outgoing SIP message it sends to the I-CSCF, and/or it may generate a pointer/reference to that data structure. If the LNG generates a pointer/reference to an Additional Data structure, it must also support deference requests for Additional Data.

### 7.2.8 Emergency Call Routing Function (ECRF)

The Emergency Call Routing Function (ECRF) is a Functional Element that exists outside of the IMS-based NG9-1-1 Emergency Services Network. The LNG queries this Functional Element using the Location-to-Service Translation (LoST) protocol defined in IETF RFC 5222 [Ref 6] to obtain routing information for an emergency origination. The ECRF maps location information (either civic address or geo-coordinates) and a Service URN provided by the LNG in the routing query to a URI associated with an I-CSCF in the IMS-based NG9-1-1 Emergency Services Network. The ECRF is out of scope for this standard. The LPG or an i3 PSAP may query the ECRF (using the LoST protocol) to obtain the identity of the transfer-to party associated with a transfer request. In addition, an i3 PSAP may send a LoST query to an ECRF to identify the URI(s) associated with the Service/Agency Locator Record Store(s) that are applicable for the location about which the PSAP is seeking agency/service-related information. The Service/Agency Locator Record includes interface points associated with the Service/Agency, such as the URI to which incident information (e.g., in the form of an Emergency Incident Data Object [EIDO]) can be directed, as well as other agency-related information.

### 7.2.9 Legacy PSAP Gateway (LPG)

The LPG is a signaling and media interconnection point between the IMS-based NG9-1-1 Emergency Services Network and legacy PSAPs. The LPG is responsible for interworking the SIP signaling that it receives from the IMS-based NG9-1-1 Emergency Services Network to the Traditional MF or Enhanced MF (E-MF) signaling supported by the legacy PSAP. The LPG is also responsible for providing emergency services-specific processing associated with transfer requests to and from legacy PSAPs, and for processing and responding to location queries from legacy PSAPs. The LPG also supports dereference interfaces that allow it to send dereference requests to the appropriate elements to obtain LbyV and Additional Data (including Emergency Incident Data Objects [EIDOs]) “by-value” when presented with the associated reference URIs in incoming SIP signaling. The LPG may query the ECRF to obtain the identity of the transfer-to party when a transfer request is received from a transfer-from legacy PSAP. See Clause 8.8.2.1.3 for further details on use of the ECRF. Note that for initial call setup, the LPG does not need to query the ECRF for routing the call to an appropriate PSAP since all necessary information for call routing to an appropriate PSAP is provided to the LPG in the initial INVITE message.

### 7.2.10 Application Server (AS)

The Application Server (AS) is used here as defined in 3GPP TS 23.002 [Ref 4] and 3GPP TS 24.147 [Ref 11] and its applicability is extended in this standard.

The AS receives SIP-based conference establishment requests from the I-CSCF and interacts with a Multimedia Resource Function Controller (MRFC) to support the conferencing and transfer of emergency calls between PSAPs served by the IMS-based NG9-1-1 Emergency Services Network.

A specialized AS, referred to as a Secure Telephone Identity Authentication Service (STI-AS), will receive SIP INVITE messages associated with callback calls from a Transit Function, or HTTP signing requests from an exit IBCF requesting the application of caller ID authentication as well as RPH and SIP Priority header signing. The STI-AS is responsible for cryptographically signing the Personal Assertion Token (PASSporT) as defined in RFC 8225 [37] and extended as defined in RFC 8443 [Ref 38] and inserting Identity header fields per RFC 8224 [Ref 36] in the SIP INVITE message returned to the Transit Function or identityHeader parameters in HTTP signing responses returned to the exit IBCF. See Clause 7.3.2 for further discussion.

A specialized AS, referred to as a Secure Telephone Identity Verification Service (STI-VS), will receive an HTTP verificationRequest from an entry IBCF associated with a 9-1-1 call, requesting verification of the Identity headers associated with a signed caller ID and RPH (if present). The STI-VS is responsible for determining the validity of the certificate referenced in the identityHeader and identityHeaders parameters as well as following the RFC 8224 [Ref 36] -defined verification procedures to check the corresponding date, originating identity (i.e., the originating telephone number) and destination identity, in the verificationRequest. The STI-VS conveys the verification result to the IBCF by including “verstatValue” and “verstatPriority” parameters in the verificationResponse. See Clause 7.3.1 for further discussion.

### 7.2.11 Multimedia Resource Function Controller (MRFC)

The Multimedia Resource Function Controller (MRFC) is used here as defined in 3GPP TS 23.002 [Ref 4] and 3GPP TS 24.147 [Ref 11] and its applicability is extended in this standard.

The MRFC Interprets information coming from an AS and controls the media stream resources in the Multimedia Resource Function Processor (MRFP) to support the conferencing and transfer of emergency calls between PSAPs served by the IMS-based NG9-1-1 Emergency Services Network.

### 7.2.12 Multimedia Resource Function Processor (MRFP)

The Multimedia Resource Function Processor (MRFP) is used here as defined in 3GPP TS 23.002 [Ref 4] and 3GPP TS 24.147 [Ref 11] and its applicability is extended in this standard.

The MRFP provides resources to be controlled by the MRFC to support the conferencing and transfer of emergency calls between PSAPs served by the IMS-based NG9-1-1 Emergency Services Network. In the context of emergency call conferencing/ transfer, the MRFC provides the mixing of incoming media streams associated with multiple parties.

### 7.2.13 Transit Function (TRF)

The Transit Function is used here as defined in 3GPP TS 23.228 [Ref 19] and its applicability is extended in this standard. As described in 3GPP TS 23.228 [Ref 19], a Transit Function is an element that determines where to route a session based on an analysis of the destination address. This includes routing to destinations in other IMS networks or the PSTN. A Transit Function may also be used by an AS if the AS does not support routing capabilities.

Under these circumstances, an AS may forward an originating request to the Transit Function and the Transit Function will route the session initiation request to the destination. 3GPP allows the Transit Function to reside in a stand-alone entity or to be combined with the functionality of a Media Gateway Control Function (MGCF), a Breakout Gateway Control Function (BGCF), a Serving Call Session Control Function (S-CSCF), or an IBCF. In the context of the IMS-based NG9-1-1 Service Architecture, the Transit Function will be used to support multimedia callbacks. If the Transit Function is operating in an NG9-1-1 Emergency Services Network that supports caller identity authentication and RPH and Priority header signing using the architecture described in Clause 7.3.2.1, the Transit Function will also be responsible for interacting with an STI-AS. The Transit Function may also be used, as an operator option, to support transfer scenarios where an AS has to initiate signaling toward a transfer-to PSAP that is outside of the IMS-based Next Generation Emergency Services Network.

## *7.3 Support for Secure Telephone Identity (STI) Services*

The Secure Telephone Identity is defined as the identity provided in a SIP Identity header field, constructed and formatted as per RFC 8224 [Ref 36]. When present, it is used to validate the identity of the calling party. In the context of the IMS-based NG9-1-1 Service Architecture, the Secure Telephone Identity Authentication Service (STI-AS) is a SIP application server that provides caller identity assertion for callbacks and other PSAP-originated outbound calls. It performs the function of the authentication service defined in RFC 8224 [Ref 36]. In the context of callback calls, the STI-AS will also be expected to perform Resource-Priority Header (RPH) and SIP Priority header signing. The STI-AS should either itself be highly secured and contain the Secure Key Store (SKS) of secret private key(s) or have an authenticated, Transport Layer Security (TLS)-encrypted interface to the SKS that stores the secret private key(s) used to create Personal Assertion Token (PASSporT) signatures. The STI-AS must be invoked after originating call processing has been applied to a callback call.

The Secure Telephone Identity Verification Service (STI-VS) is an application server that performs the function of the verification service defined in RFC 8224 [Ref 36]. It interfaces with the Secure Telephone Identity Certificate Repository to retrieve the provider public key certificate. In the context of the IMS-based NG9-1-1 Service Architecture, the STI-VS provides verification services applicable to emergency calls destined for PSAPs that are served by an IMS-based NG9-1-1 Emergency Services Network. The STI-VS must be invoked prior to terminating call processing associated with the emergency call.

The STI-AS and STI-VS are part of the Signature-based Handling of Asserted information using toKENs (SHAKEN) framework reference architecture defined in ATIS-1000074 [Ref 39]. The SHAKEN reference architecture specified in ATIS-1000074 [Ref 39] also includes the Call Validation Treatment (CVT) and SKS elements. CVT is a logical function that could be an application server function or a third-party application for applying call analytics and anti-spoofing mitigation techniques once the signature is positively or negatively verified.

The STI SKS provides highly secure storage for private keys that are used to cryptographically sign information conveyed in SIP INVITE messages presented to the STI-AS. The SKS interacts with, or is part of, the STI-AS. ATIS-1000074 [Ref 39] provides a high-level view of the SKS, with further details related to the management of STI certificate/key management provided in ATIS-1000080 [Ref 40]. In support of emergency callback, the SKS shall store keys in a FIPS-PUB-140-2 [Ref 43] level 3 or higher key store. Certificates for signing keys shall be signed directly by the root key.

For emergency originations, the STI-VS provides the results of the verification process to downstream entities to help detect potential telephone scams using spoofed telephone numbers such as SWATting, prank calls and illegitimate robocalling.

For PSAP-originated callback calls, the STI-AS asserts and cryptographically signs the telephone identity of the caller, allowing PSAP-originated calls to be validated by the networks these calls transit through (if they support such capabilities), and for the home network performing the verification to present the called party with an indication of the validity of the calling telephone number (if it supports such capabilities). Calls that contain a marking of “psap-callback” in the Priority header as well as a validated telephone identity have a higher chance of completing at the called party, which is an important feature for emergency callbacks. Note that the STI-AS will also be responsible for signing the RPH and SIP Priority header associated with a callback call. See Clause 7.4 for further discussion.

### 7.3.1 STI Verification of 9-1-1 Originations

As illustrated in the reference architecture depicted in Figure 7-3, the STI-VS accessed by the ingress IBCF in the IMS-based NG9-1-1 Emergency Services Network supports caller identity verification for emergency 9-1-1 originations presented to the IMS-based NG9-1-1 Emergency Services Network. The STI-VS interacts with the ingress IBCF for inbound emergency calls.

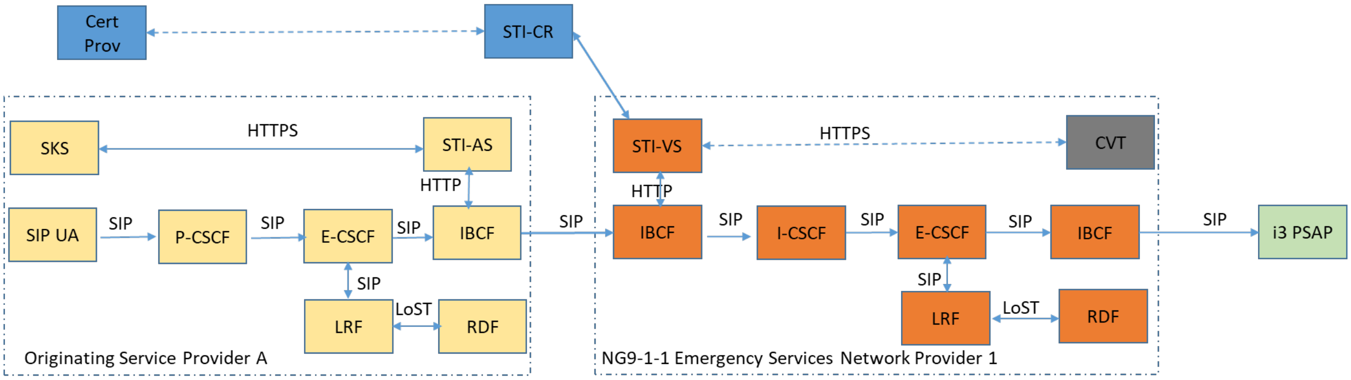


**Figure 7-3: Reference Architecture Supporting STI Verification by IMS-based NG9-1-1 Emergency Services Network**

The STI-VS is invoked by the ingress IBCF before terminating call processing has been applied, that is, before the IBCF passes the emergency call to the I-CSCF.

Upon receiving a 9-1-1 origination with an Identity header field populated as per RFC 8224 [Ref 36], the IBCF at the entry point of the IMS-based NG9-1-1 Emergency Services network shall interact with an STI-VS which will apply the procedures specified in ATIS-1000074 [Ref 39] and 3GPP TS 24.229 [Ref 2] , with the following clarifications.

- A “dest” claim in the PASSporT (within the received Identity header) that contains a service URN in the ‘sos’ family, which will be of type “uri” shall be validated using the To header field uri, normalized as specified in RFC 8224 [Ref 36], and the URN-equivalence procedures defined in RFC 8141 [Ref 52].
- If the “to” parameter received by the STI-VS in the verificationRequest message contains a URI that can be interpreted as “911” or an sos service urn (e.g., urn:service:sos), the content of the “to” parameter in the received verificationRequest does not match the “dest” claim in the PASSporT, and the “dest” claim in the PASSporT is something other than a URI that can be interpreted as “911” or an sos service URN, the “dest” claim verification shall be considered failed;
- If the “to” parameter received by the STI-VS in the verificationRequest message contains a URI that can be interpreted as “911” or an sos service urn (e.g., urn:service:sos), the content of the “to” parameter in the received verificationRequest does not match the “dest” claim in the PASSporT, and the “dest” claim in the PASSporT contains a URI that can be interpreted as “911” or an sos service URN, the “dest” claim verification shall be considered passed;
- If the “dest” claim, which contains the content of the Request-URI from the incoming SIP INVITE message, and “to” parameter, which contains the content of the To header from the SIP INVITE message contain a URI that can be interpreted to be “911”, the “dest” claim verification procedure shall be considered passed if a match is found;
- If the “dest” claim in the verificationRequest contains a service URN (e.g., urn:service:sos)  and the “to” parameter contains a URI that can be interpreted to be “911”, the “dest” claim verification procedure shall be considered passed;
- If the “dest” claim and the “to” parameter in the verificationRequest contain a service URN (e.g., urn:service:sos) , the “dest” claim verification procedure shall be performed and considered passed if a match is found;

- With regard to “orig” claim validation, if the call is to an emergency services destination, and the calling TN identified in the P-Asserted-Identity or From header field is a non-dialable callback number formatted as described in Annex C of J-STD-036-C-2 [Ref 7], then the calling TN shall be treated as if it were an E.164 number; i.e., the calling TN will be canonicalized to remove any leading “+” sign or visual separators (i.e., “.”, “-“, “(“, and “)”), and the resulting digit-string used to check the “orig” claim. This special procedure shall be applied only if the non-dialable callback number is a digit-string of 10 digits with leading digits “911” or 11 digits with leading digits " “1911”.
- Emergency 9-1-1 calls must always be progressed forward regardless of the success or failure of the verification process. If the verification request is unsuccessful, the STI-VS must return an HTTP response code in the 4xx or 5xx series, as appropriate for the error condition.

After verifying the signature in the Identity header associated with the caller identity, which validates the calling identity used when signing this information in the originating service provider STI-AS, the STI-VS may invoke the CVT (based on operator policy). The CVT is an optional function that can be invoked to perform call analytics or other spam mitigation techniques. The CVT may be integrated in the NG9-1-1 Emergency Services Network or may be provided by a third party outside the network. The functions and interfaces supported by the CVT are left to implementation.

The STI-VS must include a “verstatValue” parameter in the HTTP verificationResponse message returned to the IBCF to convey the results of the caller identity verification and may include another appropriate indicator (not defined in this document) based on interactions with the CVT. Note that the verificationResponse will include a separate verification status value in a “verstatPriority” parameter to convey RPH verification success/failure. (See Clause 7.4 for further details related to RPH signing/verification.) The IBCF shall continue processing the call as per its normal procedures by forwarding the call to the I-CSCF. The IBCF shall include a Priority-Verstat header, populated based on the content of the “verstatPriority” parameter returned in the verificationResponse, in the SIP INVITE message sent to the I-CSCF.

### 7.3.2 STI Authentication of PSAP-Originated/Callback Calls

This standard describes two alternative reference architectures for applying caller identity authentication and RPH and SIP Priority header signing to callback calls. Clause 7.3.2.1 describes an architecture in which the Transit Function in the IMS-based NG9-1-1 Emergency Services Network is responsible for interacting with the STI-AS by forwarding the SIP INVITE associated with the callback call to the STI-AS. Clause 7.3.2.2 describes an alternative architecture in which the exit point IBCF is responsible for interacting with the STI-AS via the Ms reference point, using the HTTP interface described in Annex V of 3GPP TS 24.229 [Ref 2].

#### 7.3.2.1 Transit Function Interacts with STI-AS

As illustrated in Figure 7-4, the STI-AS is accessed by the Transit Function in the IMS-based NG9-1-1 Emergency Services Network to support caller identity authentication and RPH and SIP Priority header signing (see Clause 7.4) for callback calls presented to the IMS-based NG9-1-1 Emergency Services Network. While Figure 7-4 shows the entry IBCF in the emergency caller’s home network interacting with an STI-VS using HTTP, an alternative callback architecture, where a CSCF in the emergency caller’s home network interacts with the STI-VS using SIP, is also possible.

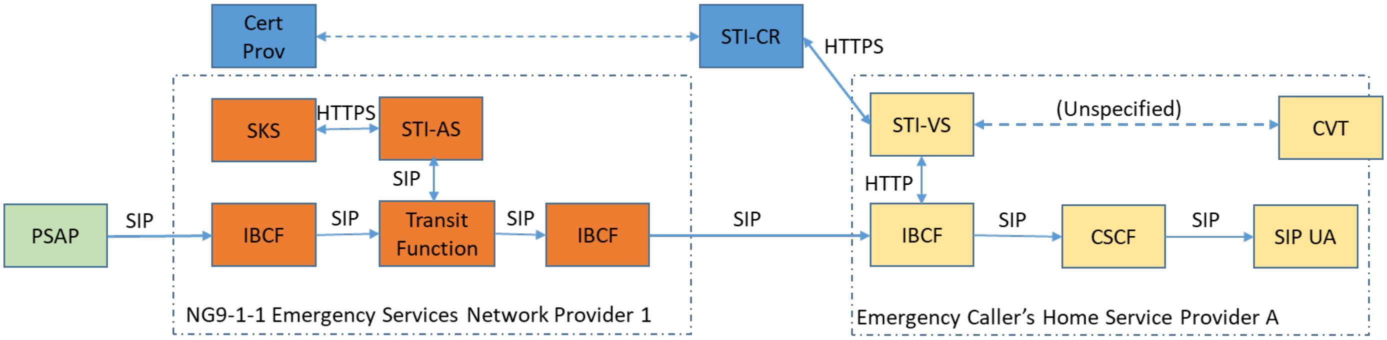


**Figure 7-4: Reference Architecture Supporting STI Authentication of Callback Calls by a Transit Function in an IMS-based NG9-1-1 Emergency Services Network**

As described in Clause 8.11, the Transit Function in an IMS-based NG9-1-1 Emergency Services Network is responsible for handling calls originated by i3 PSAPs that are routed over their serving NG9-1-1 Emergency Services Network. The Transit Function routes callback calls via an exit point IBCF to an interconnected network, which will ultimately forward the call toward the emergency caller's device, possibly via one or more other networks. The Transit Function must support callback calls with all media types, as specified in Clause 5. As described in Clause 8.11, callback calls will be marked with the value "psap-callback" in the Priority header field as documented in RFC 7090 [Ref 41].

Based on the architecture illustrated in Figure 7-4, a Transit Function processing a SIP INVITE associated with a callback call, constructed as described in Clause 8.11, shall interact with the STI-AS to assert the telephone identity of the caller (i.e., a P-Asserted-Identity header field containing sip:TN@<psapdomain>;user=phone, where the TN is associated with the PSAP originating the callback call). The Transit Function shall utilize a SIP interface to the STI-AS for the purpose of asserting and digitally signing the telephone identity (i.e., the telephone number) of PSAP-originated callback calls. The Transit Function shall invoke the STI-AS for callback calls presented to it after call processing has completed, that is, after the destination interconnected network has been determined.

Once the assertion and signing process is completed, the Transit Function shall receive the INVITE back from the STI-AS with an added SIP Identity header field (associated with the calling identity) constructed per RFC 8224 [Ref 36], using the IMS-based NG9-1-1 Emergency Services Network provider's credentials as the signing authority for the PSAP telephone identity. An Identity header associated with the RPH and SIP Priority header will also be returned. See Clause 7.4 for further details. (Note that the INVITE message received back from the STI-AS must be constructed in such a way that the Transit Function will recognize it as a "spiral" as defined in RFC 3261 [Ref 18], if the Transit Function has loop detection enabled.)

After receiving the SIP INVITE from the STI-AS, the Transit Function shall route the call to the egress IBCF. The egress IBCF shall then route the call over the Network-to-Network Interface (NNI) through the standard inter-domain routing configuration toward the entry IBCF associated with the emergency caller's home network. The home network shall perform STI verification using the procedure described in Clause 7.3.1 (assuming it supports such capabilities), and present the called UE (i.e., the UE associated with the emergency caller) with an indication of the validity of the calling telephone number, as well as the RPH and SIP Priority header (see Clause 7.4). Calls that contain a marking of "psap-callback" along with a validated telephone identity have a higher chance of completing at the called party, which is an important feature for emergency callbacks.

### 7.3.2.2 Exit Point IBCF Interacts with the STI-AS

As illustrated in Figure 7-5, the STI-AS is accessed by the exit point IBCF in the IMS-based NG9-1-1 Emergency Services Network to support caller identity authentication for callback calls presented to the IMS-based NG9-1-1 Emergency Services Network. Figure 7-5 shows the entry IBCF in the emergency caller's home network interacting with an STI-VS using HTTP. As with Figure 7-4, an alternative callback architecture, where a CSCF in the emergency caller's home network interacts with the STI-VS using SIP, is also possible.

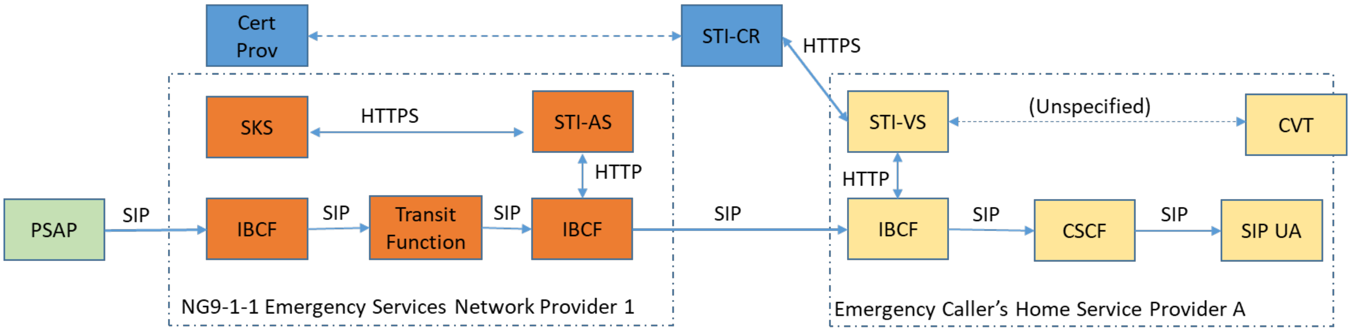


**Figure 7-5: Reference Architecture Supporting STI Authentication of Callback Calls by Exit Point IBCF in an IMS-based NG9-1-1 Emergency Services Network**

Based on the architecture illustrated in Figure 7-5, upon receiving a SIP INVITE message from a Transit Function that is associated with a callback call and that contains no Identity header, the exit point IBCF shall send an HTTP POST containing two signing requests over the Ms reference point to the STI-AS. One signingRequest asserts the telephone identity of the caller (i.e., a P-Asserted-Identity header field containing sip:TN@<psapdomain>;user=phone, where the TN is associated with the PSAP originating the callback call). That signingRequest shall include an "attest" parameter that contains the attestation information determined via local policy or received by the IBCF in an Attestation-Info header in the SIP INVITE, as well as other PASSporT information (i.e., "orig", "dest", iat and origid). A second signingRequest shall include an "rph" claim that contains an "auth" key with an assertion of "esnet.0" and an "sph" claim with a value of "psap-callback". The IBCF shall populate the assertion values in the "rph" and "sph" claims based on the content of the RPH and SIP Priority header fields received in the SIP INVITE message. The IBCF shall send the signing requests to the STI-AS for callback calls presented to it after call processing has completed, that is, after the interconnecting network has been determined.

Once the assertion and signing process is completed, using the IMS-based NG9-1-1 Emergency Services Network provider's credentials as the signing authority for the PSAP telephone identity, the IBCF shall receive an HTTP 200 OK message that contains a signingResponse with a signed identityHeader field value for the caller identity and a signingResponse that contains the signed identityHeader field value for the RPH and SIP Priority header. (See Clause 7.4 for further details related to RPH and SIP Priority header signing.)

After receiving the signing responses from the STI-AS, the egress IBCF shall populate Identity headers in the outgoing SIP INVITE message based on the identityHeader parameters in the signing responses and shall route the call over the NNI through the standard inter-domain routing configuration toward the entry IBCF associated with the emergency caller's home network. The home network shall perform STI verification using the procedure described in Clause 7.3.1 (assuming it supports such capabilities), and present the called UE (i.e., the UE associated with the emergency caller) with an indication of the validity of the calling telephone number as well as the RPH and Priority header (see Clause 7.4).

## *7.4 Resource-Priority Header Signing and SIP Priority Header Signing*

In addition to caller identity authentication/verification, 9-1-1 calls and callback calls may also be subject to Resource-Priority Header (RPH) signing. Callback calls may also be subject to SIP Priority header signing. In the context of 9-1-1 calls, a signed RPH received in an incoming INVITE message will convey to the IMS-based NG9-1-1 Emergency Services Network provider that they can trust that the RPH was populated by the originating service provider, as opposed to being inserted by a threat agent. In the context of callback calls, a signed RPH and SIP Priority header would indicate that the IMS-based NG9-1-1 Emergency Services Network provider asserts that they recognize the call is a callback call and that an RPH value in the 'esnet' namespace and a SIP Priority header set to "psap-callback" are appropriate. The SHAKEN model specified in ATIS-1000074 [Ref 39] can be leveraged to cryptographically sign and verify the SIP RPH field in SIP INVITE messages associated with 9-1-1 and callback calls, and the SIP Priority header field associated with callback calls, using the PASSporT extension defined in IETF RFC 8443 [Ref 38], the assertion values specified in IETF RFC 9027 [Ref 44], the procedures specified in ATIS-1000098 [Ref 57], and the associated Secure Telephone Identity (STI) protocols.

Specifically, this standard uses the PASSporT "rph" extension specified in IETF RFC 8443 [Ref 38], and the values for asserting an RPH associated with a 9-1-1 call and a callback call and the SIP Priority header associated with a callback call described in IETF RFC 9027 [Ref 44]. This standard also uses the STI protocols for cryptographic signing of the SIP RPH and SIP Priority header fields in support of callback calls. IETF RFC 8443 [Ref 38] extends the PASSporT specification defined in RFC 8225 [Ref 37] to allow the inclusion of cryptographically signed assertions for the values populated in the SIP RPH. The SIP RPH may be used to influence the prioritization of network resources that support communications sessions (e.g., in times of network congestion). IETF RFC 9027 [Ref 44] also supports the cryptographic signing of the SIP Priority header (in combination with the SIP RPH). The SIP Priority header may be used to influence the processing of callback calls (e.g., to bypass features that might interfere with the completion of a callback call). Like caller identity information, the RPH and SIP Priority header fields could be spoofed by unauthorized entities, leading to the misuse of network resources or undesired call routing or treatment. RFC 8443 [Ref 38] supports PASSporT extensions that will allow the cryptographic signing of the SIP RPH and the conveyance and assertion of authorization for the SIP RPH. IETF RFC 9027 [Ref 44] supports the inclusion of an "sph" claim in an "rph" PASSporT, allowing the SIP Priority header to also be signed.

In the context of emergency (9-1-1) calling, the extension to the PASSporT to assert an RPH value in the 'esnet' namespace will be in addition to the PASSporT object that is used for caller identity attestation. Specifically, assertion of the information in the RPH will involve the inclusion of a "ppt" extension with an "rph" claim in the PASSporT. Based on RFC 8443 [Ref 38], a PASSporT header with the "ppt" extension will consist of the following information:

```
{
  "typ":"passport",
  "ppt":"rph",
  "alg":"ES256",
  "x5u":"https://www.example.org/cert.cer"
}
```

The syntax to be used with an "rph" claim for a SIP RPH that is associated with an emergency (9-1-1) origination, as well as an "rph" claim for a SIP RPH that is associated with a callback call is provided in IETF RFC 9027 [Ref 44]. IETF RFC 9027 [Ref 44] adds new assertion values for the Resource-Priority Header ("rph") claim defined in RFC 8443 [Ref 38], in support of Emergency Services Networks for emergency call origination and callback.

The following is an example of an "rph" claim for a SIP 'Resource-Priority' header field to be used with an emergency (9-1-1) origination:

```
{
   "orig":{"tn":"12155551212"},
   "dest":{"uri":["urn:service:sos"]},
   "iat":1443208345,
   "rph":{"auth":["esnet.1"]}
 }
```

After the header and claims PASSporT objects have been constructed, their signature is generated normally per the guidance in RFC 8225 [Ref 37] using the full form of PASSporT.

SIP RPH signing does not change or modify 9-1-1 call processing, signaling and routing procedures; it simply provides a security tool for a receiving provider to determine if the SIP RPH is trusted. Upon receiving a SIP INVITE associated with an emergency (9-1-1) origination that contains two Identity headers (one associated with caller identity authentication and one associated with RPH signing), and prior to terminating call processing associated with the emergency call (that is, before the entry IBCF in the IMS-based NG9-1-1 Emergency Services Network forwards the emergency call to the I-CSCF), the IBCF shall interact with the verification service.

As for caller identity verification, when performing verification of the signed RPH, the terminating STI-VS shall retrieve the certificate referenced by the "x5u" field in the PASSporT protected header from the STI Certificate Repository (STI-CR). The STI-VS shall validate the certificate and then extract the public key as per ATIS-1000074 [Ref 39]. The STI-VS shall use the public key to verify the signature in the Identity header fields, which validates the RPH field used when the originating service provider STI-AS signed the RPH.

Regardless of the result of the RPH verification process, the STI-VS shall pass the results back to the IBCF in a "verstatPriority" parameter within an HTTP verificationResponse. In the context of an emergency (9-1-1) origination, the values for the "verstatPriority" associated with RPH verification success/failure include: "RPH-Validation-Passed", "RPH-Validation-Failed", or "No-RPH-Validation". Once the IBCF receives the verificationResponse from the STI-VS, it will proceed with processing the emergency call. The IBCF shall convey the RPH verification results downstream by including a Priority-Verstat header field in the outgoing SIP INVITE. The Priority-Verstat header field will contain the content of the "verstatPriority" parameter returned by the STI-VS in the verificationResponse.

In the context of callback call processing using the architecture illustrated in Figure 7-4, upon receiving a SIP INVITE associated with a callback call, the Transit Function shall interact with the STI-AS by passing it the SIP INVITE. As described in Clause 7.3.2.1, the Transit Function shall invoke the STI-AS for callback calls presented to it after call processing has completed, that is, after the destination interconnected network has been determined to be an IP network. The STI-AS shall determine, through service provider-specific means, the legitimacy of the caller identity as well as the content of the RPH field (i.e., the ‘esnet’ namespace value) and the SIP Priority header field (i.e., the value “psap-callback”) being used in the INVITE. The STI-AS shall then securely request its private key from the SKS. The SKS provides the private key in the response, and the STI-AS shall sign the caller identity and RPH/SIP Priority header in the INVITE and add two Identity headers, one associated with the caller identity and one associated with the signed RPH/SIP Priority header. In creating the Identity header associated with the RPH/SIP Priority header, the standard PASSporT extension for “rph” shall be used as defined in IETF RFC 8443 [Ref 38], including the “sph” claim. IETF RFC 8443 [Ref 38] defines a JavaScript Object Notation (JSON) Web Token claim for "rph" which provides an assertion for the information in the SIP 'Resource-Priority' header field. The “rph” PASSporT extension shall also include an “sph” claim, as defined in IETF RFC 9027 [Ref 44].

In the context of callback call processing using the architecture illustrated in Figure 7-5, upon receiving a SIP INVITE associated with a callback call, the Transit Function shall determine the target interconnected network, and if that network is an IP network, pass the call to an exit IBCF. The exit IBCF shall send an HTTP POST containing two signing requests to the STI-AS. As described in Clause 7.3.2.2, the IBCF shall invoke the STI-AS for callback calls presented to it after call processing has completed, that is, after the Transit Function has determined that the destination interconnected network is an IP network. The STI-AS shall determine, through service provider-specific means, the legitimacy of the caller identity as well as the content of the RPH field (i.e., the ‘esnet’ namespace value) and SIP Priority header (i.e., the value “psap-callback”) included in the signing requests. The STI-AS shall then securely request its private key from the SKS. The SKS shall provide the private key in the response, and the STI-AS shall sign the caller identity and RPH/SIP Priority header. The STI-AS shall then include two signing responses, one associated with the caller identity and one associated with the signed RPH/SIP Priority header, in the HTTP 200 OK that it returns to the exit IBCF. Each signingResponse shall contain an identityHeader parameter. In creating the identityHeader parameter associated with the RPH/SIP Priority header, the standard PASSporT extension for “rph” shall be used as defined in IETF RFC 8443 [Ref 38]. IETF RFC 8443 [Ref 38] defines a JSON Web Token claim for "rph" which provides an assertion for the information in SIP 'Resource-Priority' header field. The “rph” PASSporT extension will also include an “sph” claim, as defined in IETF RFC 9027 [Ref 44].

The authentication service signs the value of the PASSporT claim by verifying the asserted RPH value and the SIP Priority header value. It adds a "ppt" value of "rph" to the header of the PASSporT object. A PASSporT header with the "ppt" included will look as follows:

```
{
    "typ":"passport",
    "ppt":"rph",
    "alg":"ES256",
    "x5u":"https://www.example.org/cert.cer"
  }
```

The "rph" claim will provide an assertion of the value provided in the SIP "Resource-Priority" header field. Specifically, the "rph" claim includes an assertion of the priority level to be used for a given communication session. As indicated above, the syntax to be used for an “rph” claim associated with a callback call is addressed in IETF RFC 9027 [Ref 44]. The “rph” PASSporT will also include an “sph” claim asserting the value of the SIP Priority header.

The following is an example of an "rph" claim for a SIP 'Resource-Priority' header field with an assertion of “esnet.0”, and a SIP Priority header field with a “psap-callback” value associated with a callback call:

```
{
  "orig":{"tn":"12155551213"},
  "dest":{"tn":["12155551212"]},
  "iat":1443208345,
  "rph":{"auth":["esnet.0"]}
   "sph":"psap-callback"
}
```

After the header and claims PASSporT objects have been constructed, their signature is generated normally per IETF RFC 8225 [Ref 37] using the full form of PASSporT.

If the architecture described in Clause 7.3.2.1 is used, the STI-AS shall pass the INVITE with the Identity headers back to the Transit Function. The Transit Function shall apply standard resolution and route the call to the egress IBCF. If the architecture described in Clause 7.3.2.2 is used, the STI-AS shall return an HTTP 200 OK message containing two signing responses, each with an identityHeader parameter, back to the exit point IBCF. The exit point IBCF shall use the identityHeader parameters to populate Identity headers in the outgoing SIP INVITE message. The SIP INVITE is routed over the NNI through the standard inter-domain routing configuration toward the entry IBCF associated with the emergency caller's home network.

## *7.5 Reference Protocols*

This clause defines the protocols in the IMS-based NG9-1-1 Service Architecture. It defines specific protocols and differences from those defined in 3GPP TS 23.167 [Ref 1].

Figure 7-2 illustrates the architecture for location acquisition and routing for emergency services. The following functional elements and associated reference points are illustrated:

- *E-CSCF to LRF Reference Point (Ml)*

  The Ml interface is defined in 3GPP TS 23.167 [Ref 1] and expanded upon in Clauses 5.11 and 5.12 of 3GPP TS 24.229 [Ref 2]. The LRF operates as a SIP redirecting server to the E-CSCF. The E-CSCF sends a SIP INVITE to the LRF passing sufficient information in the headers and/or body to allow the LRF to acquire location if necessary and determine routing (via the RDF). The LRF responds with a SIP 300 Multiple Choices response containing routing information.

- *LRF to RDF Reference Point (R0)*

  The R0 Reference point is used by the LRF to obtain routing URIs from the RDF. The protocol between the LRF and the RDF is the Location to Service Translation Protocol (LoST) [Ref 6]. Using this protocol, the location and the service URN are sent to the RDF and a routing URI is returned. The LoST messages of findService and findServiceResponse are used. It is assumed that the RDF returns a SIP URI in all cases, regardless of the destination (i.e., legacy or NENA i3 PSAP).

- *LRF to LS Reference Point (D1)*

  The D1 Reference Point is specific to location acquisition for call routing where the emergency call request contains a location reference and the LRF has to query the IP Originating Service Provider network. The protocol used on the D1 Reference Point is the Dereferencing Protocol using HTTP Enabled Location Protocol (HELD) [Ref 9]. The messages of locationRequest and locationResponse are used. The use of SIP SUBSCRIBE/NOTIFY is for future study.

- *LRF to LNG Reference Point (D2)*

  The D2 Reference Point is specific to location acquisition for call routing where the emergency call request contains a location reference and the LRF has to query the LNG. The protocol used on the D2 Reference Point is the Dereferencing Protocol using HTTP Enabled Location Protocol (HELD) [Ref 9]. The messages of locationRequest and locationResponse are used. The use of SIP SUBSCRIBE/NOTIFY [Ref 17] is for future study.

- *LNG to Ingress IBCF (ici)*

  The ici Reference Point is used by the LNG to deliver emergency sessions requests toward the PSAP via the IBCF. This Reference Point uses the SIP protocol.

- *Egress IBCF to LPG (ici)*

  The ici Reference Point is used by the IBCF to deliver emergency sessions requests toward the PSAP via the LPG. This Reference Point uses the SIP protocol.

- *IP OSP to Ingress IBCF (ici)*

  The ici Reference Point is used by the IP OSP to deliver emergency sessions requests toward the PSAP via the IBCF. This Reference Point uses the SIP protocol.

- *Egress IBCF to NENA i3 PSAP (ici)*

  The ici Reference Point is used by the IBCF to deliver emergency sessions requests toward the NENA i3 PSAP. This Reference Point uses the SIP protocol.

- *I-CSCF to AS Reference Point (Ma)*

  The Ma interface is defined in 3GPP TS 23.002 [Ref 4] and is used to forward SIP requests from an I-CSCF to an AS. In the context of emergency call transfer, the Ma reference point is used to forward conference establishment requests initiated by transfer-from i3 PSAPs or LPGs (on behalf of transfer-from legacy PSAPs). The protocol to be used on the Ma reference point is SIP.

- *AS to MRFC Reference Point for Media Control (Cr)*

  The Cr interface is defined in 3GPP TS 23.002 [Ref 4]. The Cr reference point allows interaction between an AS and an MRFC for media control. The Cr reference point enables media control protocol requests, responses and notifications to be sent between the MRFC and an AS. The establishment and management of the media control protocol are done via SIP messages sent between the AS and the MRFC.

- *MRFC to MRFP Reference Point (Mp)*

  The Mp interface is defined in 3GPP TS 23.002 [Ref 4]. The Mp reference point allows an MRFC to control media stream resources provided by an MRFP. The protocol for the Mp reference point is described in TS 29.333 [Ref 32].

- *IBCF to AS Reference Point (T1)*

  The T1 Reference Point supports communication between an IBCF and an AS in support of emergency call transfer between PSAPs served by an IMS-based NG9-1-1 Emergency Services Network. Once a transfer-from i3 PSAP or LPG has established a conference with a conferencing AS, subsequent requests and responses related to the transfer of an emergency call may involve direct communication between the conferencing AS and an IBCF over the T1 reference point. The protocol to be used on the T1 reference point is SIP.

- *AS to Transit Function (Mf)*

  The Mf Reference Point supports communication between an AS and a Transit Function. In the context of the IMS-based NG9-1-1 Service Architecture, the Mf Reference Point is used to support emergency call transfer, as well as the handling of callback calls. The Mf Reference Point uses the SIP protocol.

- *Transit Function to IBCF (Mx)*

  The Mx Reference Point supports the exchange of messages between an IBCF and other functional elements in an IMS network. In the context of the IMS-based NG9-1-1 Service Architecture, communication between the Transit Function and the IBCF to support emergency call transfer and callback calls utilizes SIP signaling over the Mx Reference Point.

Figures 7-3 through 7-5 related to STI authentication and verification include the following additional functional elements and associated reference point:

- *IBCF to STI-AS/STI-VS (Ms)*

  As described in Clause V.2.1 in Annex V of 3GPP TS 24.229 [Ref 2], the Ms reference point is used to request the signing of the caller identity or to request verification of a signed identity in an Identity header field. In the context of this specification, this Reference Point allows the IBCF to communicate with an AS that performs the function of the verification service (for 9-1-1 calls) and, in the context of the architecture described in Clause 7.3.2.2, the function of the authentication service (for callback calls) defined in RFC 8224 [Ref 36]. This standard supports the Release 17 extensions to Annex V of 3GPP TS 24.229 [Ref 2] related to the signing and verification of RPH and SIP Priority header content. The protocol to be used on the Ms Reference Point is HTTP.

Note that the Le Reference Point associated with the LRF, as defined in 3GPP TS 23.167 [Ref 1], is not applicable for the IMS-based NG9-1-1 Service Architecture. For call requests that contain a location reference, the NENA i3 PSAP will either query the LNG or the IP OSP network for location information. For call requests that contain a location reference, the legacy PSAP will query the LPG, which in turn will either query the LNG or the IP OSP network for location information.

See ATIS-1000074 [Ref 39] for discussion of the interfaces between the elements of the SHAKEN architecture (e.g., STI-AS to SKS, STI-VS to STI-CR).

# 8 Stage 2 Call Flows

## *8.1 Legacy Wireline Origination to i3 and Legacy PSAPs*

### 8.1.1 Delivery of Legacy Wireline Emergency Call Origination to i3 PSAP

The call flow provided in Figure 8-1 illustrates a scenario where a legacy wireline emergency call is delivered by a legacy origination network via SS7 or MF  trunks to an IMS-based NG9-1-1 Emergency Services Network.  The call is delivered to an i3 LNG on the ingress side of the IMS-based NG9-1-1 Emergency Services Network with an E.164 number as the SS7 Calling Party Number/MF ANI and the digits “911” as the called number.  This call flow assumes that the LNG will use the E.164 number to query a local location server/database that contains static TN-to-location mappings to obtain the routing/caller location for the call.  This location information is then passed “by-value” to the IMS-based NG9-1-1 Emergency Services Network. The location is used by the LRF to query the RDF for call routing information. This call flow assumes that the Route URI that is returned by the RDF is the URI associated with an i3 PSAP.  Furthermore, this call flow assumes that the call is delivered to the i3 PSAP with the LbyV that was provided to the IMS-based NG9-1-1 Emergency Services Network by the LNG, as well as Additional Data (by-value) that was provided by the LNG.

NOTE: The I-CSCF does not add itself to the Record-Route header in the call flows in Clause 8. The E-CSCF may or may not add itself to the Record-Route header (see Clause 9.1).

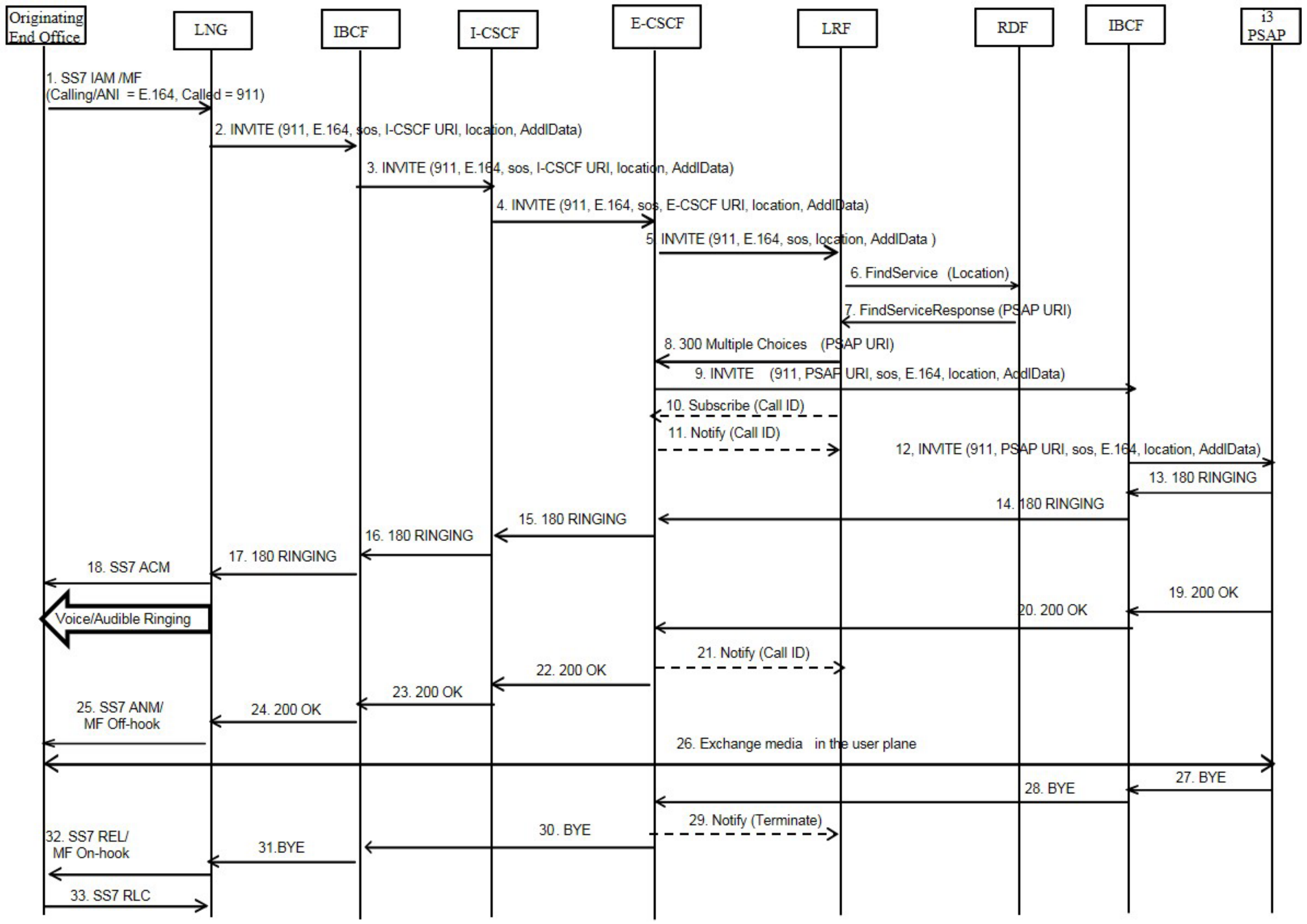

Originating End Office
LNG
IBCF
I-CSCF
E-CSCF
LRF
RDF
IBCF
i3 PSAP
1. SS7 IAM /MF (Calling/ANI = E.164, Called = 911)
2. INVITE (911, E.164, sos, I-CSCF URI, location, AddlData)
3. INVITE (911, E.164, sos, I-CSCF URI, location, AddlData)
4. INVITE (911, E.164, sos, E-CSCF URI, location, AddlData)
5. INVITE (911, E.164, sos, location, AddlData )
6. FindService (Location)
7. FindServiceResponse (PSAP URI)
8. 300 Multiple Choices (PSAP URI)
9. INVITE (911, PSAP URI, sos, E.164, location, AddlData)
10. Subscribe (Call ID)
11. Notify (Call ID)
12, INVITE (911, PSAP URI, sos, E.164, location, AddlData)
13. 180 RINGING
14. 180 RINGING
15. 180 RINGING
16. 180 RINGING
17. 180 RINGING
18. SS7 ACM
Voice/Audible Ringing
19. 200 OK
20. 200 OK
21. Notify (Call ID)
22. 200 OK
23. 200 OK
24. 200 OK
25. SS7 ANM/ MF Off-hook
26. Exchange media in the user plane
27. BYE
28. BYE
29. Notify (Terminate)
30. BYE
31.BYE
32. SS7 REL/ MF On-hook
33. SS7 RLC

**Figure 8.1: Delivery of Legacy Wireline Emergency Call Origination to i3 PSAP**

**Step 1.** The originating end office sends an emergency call origination from a legacy wireline caller to the LNG over an MF or SS7-supported trunk group. The call setup signaling includes the caller's telephone number (in E.164 format) and the digits "911".

**Step 2.** The LNG uses the E.164 number received in incoming signaling to query a local location database/server that contains static TN-to-location mappings and obtains the location for the call, as described in NENA-STA-010.3 [Ref 27]. The LNG then uses this location information to query an i3 Emergency Call Routing Function (ECRF) to obtain the Route URI associated with the I-CSCF in the IMS-based NG9-1-1 Emergency Services Network (not shown). The LNG also creates an Additional Data structure per NENA-STA-010.3 [Ref 27] and passes it forward "by-value". The LNG interworks the incoming MF/SS7 signaling to SIP, populating the calling (E.164) number in the From and PAI headers, "911" (expressed as a URI) in the To header, and a service URN of urn:service:sos in the Request-URI. The outgoing SIP INVITE message also includes a Call-Info header that contains a cid that points to the Additional Data in the body of the SIP INVITE, as well as a Geolocation header that contains a cid that points to the location information (i.e., the PIDF-LO[13]) in the body of the SIP INVITE message, and a Geolocation-Routing header set to "yes". The LNG forwards this SIP INVITE message to the (ingress) IBCF.

**Step 3.** The (ingress) IBCF forwards the SIP INVITE message to the I-CSCF.

[13] Defined in RFC 4119 [Ref 16], updated by RFC 5139 [Ref 8] and RFC 5491 [Ref 10]).

**Step 4.** The I-CSCF forwards the SIP INVITE message to the pre-configured E-CSCF. The I-CSCF does not add itself to the Record-Route header.

**Step 5.** The E-CSCF forwards the SIP INVITE to the LRF.

**Step 6.** The LRF queries the RDF with the location and the emergency service URN (urn:service:sos) received in the SIP INVITE message from the E-CSCF.

**Step 7.** The RDF returns a Route URI. In this example, the Route URI is associated with an i3 PSAP that is served by the IMS-based NG9-1-1 Emergency Services Network.

**Step 8.** The LRF redirects the call back to the E-CSCF, passing the Route (PSAP) URI.

**Step 9.** The E-CSCF generates an outgoing SIP INVITE message, using the information received from the LNG and the LRF, and forwards it to the IBCF. The SIP INVITE message contains "911" (expressed as a URI) in the To header, the PSAP URI in the Route header, the sos service URN in the Request-URI, the E.164 number in the From and P-Asserted-Identity headers, and a message body that contains the LbyV, Additional Data (by value) and the SDP. The SIP INVITE also contains a pointer to the LbyV in the Geolocation header, a Geolocation-Routing header set to "yes", and a pointer(s) to the Additional Data in the Call-Info header(s).

**Step 10.** (Optional) The LRF may subscribe to the state of the call.

**Step 11.** (Conditional on Step 10) The E-CSCF sends an initial notification of the state.

**Step 12.** The IBCF forwards the SIP INVITE to the i3 PSAP.

**Step 13.** An indication that the call taker is being alerted is returned by the i3 PSAP to the (egress) IBCF (using a SIP 180 RINGING message).

**Step 14.** The (egress) IBCF passes the SIP 180 RINGING message to the E-CSCF.

**Step 15.** The E-CSCF passes the SIP 180 RINGING message to the I-CSCF.

**Step 16.** The I-CSCF passes the SIP 180 RINGING message to the (ingress) IBCF.

**Step 17.** The (ingress) IBCF passes the SIP 180 RINGING message to the LNG.

**Step 18.** The LNG interworks the SIP 180 RINGING message to an SS7 ACM (if the call was delivered to it over an SS7-supported trunk group) and returns it to the originating end office. The LNG also generates audible ringing toward the caller.

**Step 19.** When the PSAP answers the call, it returns a SIP 200 OK message to the (egress) IBCF.

**Step 20.** The (egress) IBCF passes the SIP 200 OK message to the E-CSCF.

**Step 21.** (Conditional on Step 10) The E-CSCF sends a notification to the LRF updating the call state.

**Step 22.** The E-CSCF passes the SIP 200 OK message to the I-CSCF.

**Step 23.** The I-CSCF passes the SIP 200 OK message to the (ingress) IBCF.

**Step 24.** The (ingress) IBCF passes the SIP 200 OK message to the LNG.

**Step 25.** The LNG maps the SIP 200 OK message to an SS7 ANM message or MF off-hook signal to the originating end office.

**Step 26.** At this point a two-way connection is established between the caller and the PSAP.

**Step 27.** At some point the call is terminated. In this call flow, the PSAP terminates the call and sends a SIP BYE message to the (egress) IBCF.

**Step 28.** The SIP BYE is passed from the (egress) IBCF to the E-CSCF.

**Step 29.** (Conditional on Step 10) The E-CSCF then notifies the LRF that the call has terminated, provided the E-CSCF added itself to the Record-Route..

**Step 30.** The E-CSCF passes the SIP BYE message to the (ingress) IBCF.

**Step 31.** The (ingress) IBCF passes the SIP BYE message to the LNG.

**Step 32.** The LNG maps the SIP BYE message to an SS7 REL message or an MF on-hook indication and sends it to the originating end office.

**Step 33.** Upon receiving an SS7 REL message, the originating end office sends an SS7 RLC message to the LNG.

### 8.1.2 Delivery of Legacy Wireline Emergency Call Origination to Legacy PSAP

The call flow provided in Figure 8-2 illustrates a scenario where a legacy wireline emergency call is delivered by a legacy origination network via SS7 or MF trunks to an IMS-based NG9-1-1 Emergency Services Network. The call is delivered to an i3 LNG on the ingress side of the IMS-based NG9-1-1 Emergency Services Network with an E.164 number as the SS7 Calling Party Number/MF ANI and the digits “911” as the called number. This call flow assumes that the LNG will use the E.164 number to query a local location server/database that contains static TN-to-location mappings to obtain the routing/caller location for the call. This location information is then passed “by-value” to the IMS-based NG9-1-1 Emergency Services Network. The location is used by the LRF to query the RDF for call routing information. This call flow assumes that the Route URI that is returned by the RDF is the URI associated with a legacy PSAP, and that the call is forwarded via an IBCF to an i3 LPG with the LbyV and Additional Data (by-value) that was provided to the IMS-based NG9-1-1 Emergency Services Network by the LNG.

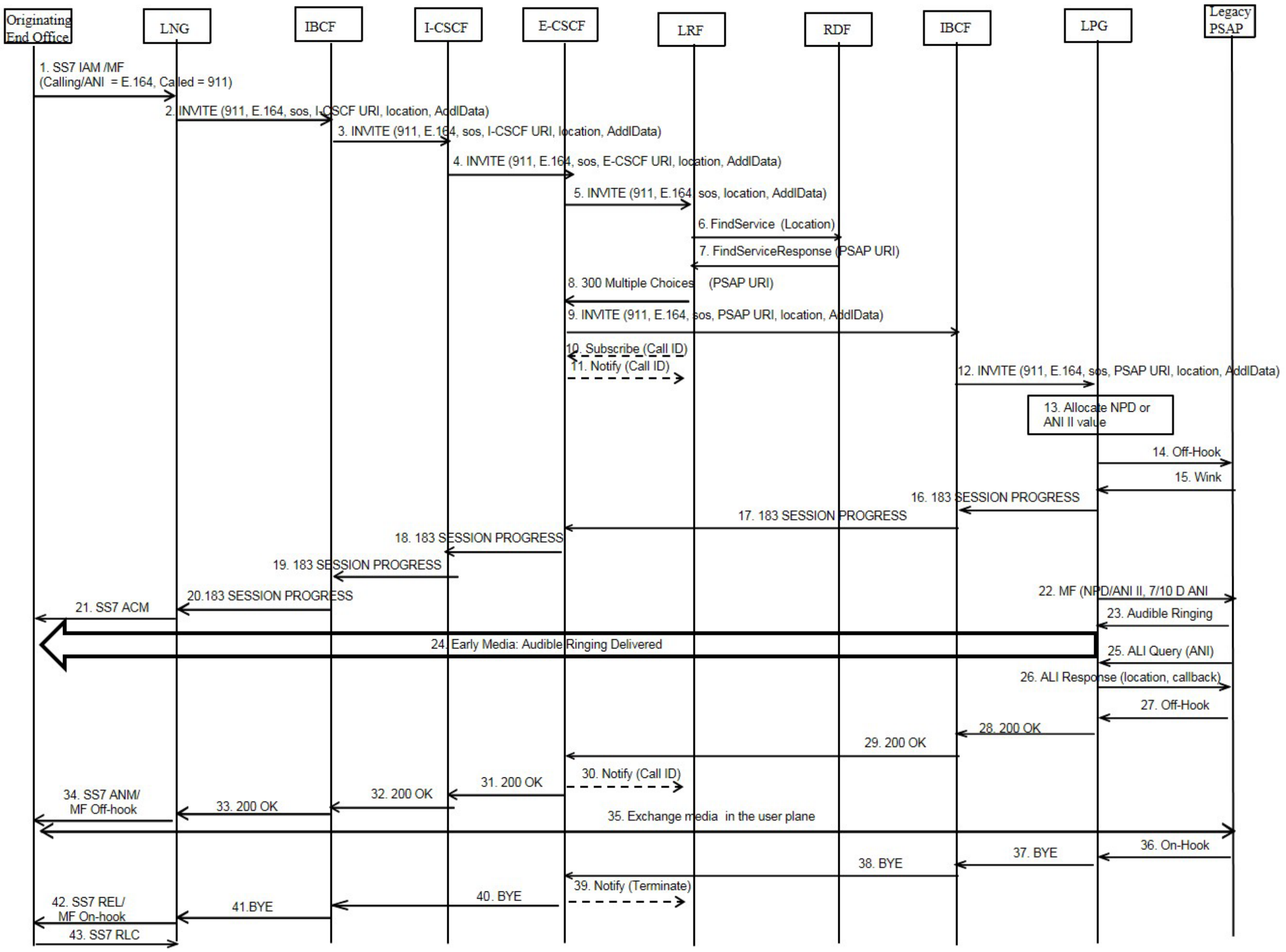

Originating End Office
LNG
IBCF
I-CSCF
E-CSCF
LRF
RDF
IBCF
LPG
Legacy PSAP
1. SS7 IAM /MF (Calling/ANI = E.164, Called = 911)
2. INVITE (911, E.164, sos, I-CSCF URI, location, AddlData)
3. INVITE (911, E.164, sos, I-CSCF URI, location, AddlData)
4. INVITE (911, E.164, sos, E-CSCF URI, location, AddlData)
5. INVITE (911, E.164 sos, location, AddlData)
6. FindService (Location)
7. FindServiceResponse (PSAP URI)
8. 300 Multiple Choices (PSAP URI)
9. INVITE (911, E.164, sos, PSAP URI, location, AddlData)
10. Subscribe (Call ID)
11. Notify (Call ID)
12. INVITE (911, E.164, sos, PSAP URI, location, AddlData)
13. Allocate NPD or ANI II value
14. Off-Hook
15. Wink
16. 183 SESSION PROGRESS
17. 183 SESSION PROGRESS
18. 183 SESSION PROGRESS
19. 183 SESSION PROGRESS
20.183 SESSION PROGRESS
21. SS7 ACM
22. MF (NPD/ANI II, 7/10 D ANI
23. Audible Ringing
24. Early Media: Audible Ringing Delivered
25. ALI Query (ANI)
26. ALI Response (location, callback)
27. Off-Hook
28. 200 OK
29. 200 OK
30. Notify (Call ID)
31. 200 OK
32. 200 OK
33. 200 OK
34. SS7 ANM/ MF Off-hook
35. Exchange media in the user plane
36. On-Hook
37. BYE
38. BYE
39. Notify (Terminate)
40. BYE
41.BYE
42. SS7 REL/ MF On-hook
43. SS7 RLC

**Figure 8.2: Delivery of Legacy Wireline Emergency Call Origination to Legacy PSAP**

**Step 1.** The originating end office sends an emergency call origination from a legacy wireline caller to the LNG over an MF or SS7-supported trunk group. The call setup signaling includes the caller's telephone number (in E.164 format) and the digits "911".

**Step 2.** The LNG uses the E.164 number received in incoming signaling to query a local location database/server that contains static TN-to-location mappings and obtains the location for the call, as described in NENA-STA-010.3 [Ref 27]. The LNG then uses this location information to query an i3 ECRF to obtain the Route URI associated with the I-CSCF in the IMS-based NG9-1-1 Emergency Services Network (not shown). The LNG also creates an Additional Data structure per NENA-STA-010.3 [Ref 27] and passes it forward "by-value". The LNG interworks the incoming MF/SS7 signaling to SIP, populating the calling (E.164) number in the From and PAI headers, "911" (expressed as a URI) in the To header, and a service URN of urn:service:sos in the Request-URI. The outgoing SIP INVITE message also contains a Call-Info header that contains a cid that points to the Additional Data in the body of the SIP INVITE, as well as a Geolocation header that contains a cid that points to the location information (i.e., the PIDF-LO) in the body of the SIP INVITE message, and a Geolocation-Routing header set to "yes". The LNG forwards this SIP INVITE message to the (ingress) IBCF.

**Step 3.** The (ingress) IBCF forwards the SIP INVITE message to the I-CSCF.

**Step 4.** The I-CSCF forwards the SIP INVITE to the pre-configured E-CSCF.

**Step 5.** The E-CSCF forwards the SIP INVITE to the LRF.

**Step 6.** The LRF queries the RDF with the location and the emergency service URN (urn:service:sos) received in the SIP INVITE message from the E-CSCF.

**Step 7.** The RDF returns a Route URI. In this example, the Route URI is associated with a legacy PSAP that is served by the IMS-based NG9-1-1 Emergency Services Network.

**Step 8.** The LRF redirects the call back to the E-CSCF, passing the Route (PSAP) URI.

**Step 9.** The E-CSCF generates an outgoing SIP INVITE message, using the information received from the LNG and the LRF, and forwards it to the (egress) IBCF. The SIP INVITE message contains the E.164 number in the From and P-Asserted-Identity headers, "911" (expressed as a URI) in the To header, the PSAP URI in the Route header, the sos service URN in the Request-URI, and a message body that contains the LbyV , Additional Data (by-value) and the SDP. The SIP INVITE also contains a pointer to the LbyV in the Geolocation header, a Geolocation-Routing header set to "yes", and a pointer(s) to the Additional Data in the Call-Info header(s).

**Step 10.** (Optional) The LRF may subscribe to the state of the call.

**Step 11.** (Conditional on Step 10) The E-CSCF sends an initial notification of the state.

**Step 12.** The (egress) IBCF forwards the SIP INVITE message to the LPG.

**Step 13.** The LPG determines, based on provisioning, whether the PSAP associated with the received PSAP URI supports a Traditional MF or Enhanced MF interface. Depending on the type of interface supported by the PSAP, the LPG assigns an appropriate NPD or ANI II value to the call.

**Step 14.** The LPG generates an off-hook signal toward the legacy PSAP.

**Step 15.** The legacy PSAP returns a wink signal back to the LPG.

**Step 16.** The LPG generates a 183 Session Progress message and sends it to the (egress) IBCF.

**Step 17.** The (egress) IBCF passes the 183 Session Progress message to the E-CSCF.

**Step 18.** The E-CSCF passes the 183 Session Progress message to the I-CSCF.

**Step 19.** The I-CSCF passes the 183 Session Progress message to the (ingress) IBCF.

**Step 20.** The (ingress) IBCF passes the 183 Session Progress message to the LNG.

**Step 21.** The LNG maps the 183 Session Progress message to an SS7 ACM (assuming that the call was received by the LNG over an SS7-supported trunk group) and passes it to the originating end office.

**Step 22.** The LPG maps the SIP signaling from the incoming INVITE message to the outgoing Traditional or Enhanced MF signaling sequences and forwards the call to the legacy PSAP. The MF signaling includes an NPD + 7-digit calling number/ANI (derived from the E.164 number received in incoming signaling) or II digits + 10-digit calling number/ANI, as appropriate for the PSAP interface.

**Step 23.** Audible ringing is returned by the legacy PSAP to the LPG.

**Step 24.** Audible ringing is passed to the originating end office/caller.

**Step 25.** The legacy PSAP sends a location query to the LPG using a NENA-defined ALI query protocol. The ALI query includes the 10-digit calling number/ANI received in Step 22. (Note that this can happen any time after Step 22.)

**Step 26.** The LPG returns an ALI response to the legacy PSAP that includes location information, a callback number and other information (e.g., class of service), as appropriate for the interface.

**Step 27.** When the PSAP answers the call, it returns an off-hook signal to the LPG.

**Step 28.** In response to the off-hook signal, the LPG generates a SIP 200 OK message and passes it to the (egress) IBCF.

**Step 29.** The (egress) IBCF passes the SIP 200 OK message to the E-CSCF.

**Step 30.** (Conditional on Step 10) The E-CSCF sends a notification to the LRF updating the call state.

**Step 31.** The E-CSCF passes the SIP 200 OK message to the I-CSCF.

**Step 32.** The I-CSCF passes the SIP 200 OK message to the (ingress) IBCF.

**Step 33.** The (ingress) IBCF passes the 200 OK message to the LNG.

**Step 34.** The LNG maps the SIP 200 OK message to an SS7 ANM message or MF off-hook signal to the originating end office.

**Step 35.** At this point a two-way connection is established between the caller and the PSAP.

**Step 36.** At some point the call is terminated. In this call flow, the PSAP terminates the call and sends an on-hook indication to the LPG.

**Step 37.** The LPG maps the on-hook indication to a SIP BYE message and sends the SIP BYE message to the (egress) IBCF.

**Step 38.** The (egress) IBCF sends the SIP BYE message to the E-CSCF.

**Step 39.** (Conditional on Step 10) The E-CSCF then notifies the LRF that the call has terminated.

**Step 40.** The E-CSCF passes the SIP BYE message to the (ingress) IBCF.

**Step 41.** The (ingress) IBCF passes the SIP BYE message to the LNG.

**Step 42.** The LNG maps the SIP BYE message to an SS7 REL message or an MF on-hook indication, as appropriate, and sends it to the originating end office.

**Step 43.** Upon receiving an SS7 REL message, the originating end office sends an SS7 RLC message to the LNG.

## *8.2 Legacy CMRS Origination to i3 and Legacy PSAPs*

### 8.2.1 Delivery of Legacy Wireless Emergency Call Origination to i3 PSAP Using WCM

The call flow provided in Figure 8-3 illustrates a scenario where a legacy wireless emergency call is delivered by a legacy origination network via SS7 or MF trunks to an IMS-based NG9-1-1 Emergency Services Network using

WCM. The call is delivered by the Mobile Switching Center (MSC) to an i3 LNG with an ESRK signaled as the SS7 Calling Party Number/MF ANI and the digits "911" as the called number. This call flow assumes that the LNG will determine the routing location for the call using local mappings based on the ESRK, and that it will also use the ESRK to query a Location Server (i.e., MPC/GMLC) in the legacy wireless network, using the E2 protocol, to obtain the caller location and callback number for the call. The LNG uses the routing location to query an ECRF (not shown) and then uses the URI provided in the ECRF response to route the call via an (ingress) IBCF to an I-CSCF in the IMS-based NG9-1-1 Emergency Services Network. The call is delivered to the IMS-based NG9-1-1 Emergency Services Network with a callback number, LbyR (i.e., a location URI), and Additional Data by reference (i.e., with a reference URI in a Call-Info header). The LRF uses the routing location and the sos service URN to query the RDF. This call flow assumes that the Route URI that is returned by the RDF is the URI associated with an i3 PSAP. The LRF returns the Route URI to the E-CSCF and the call is delivered to the i3 PSAP with location (i.e., LbyR), a callback number, and Additional Data (by reference).

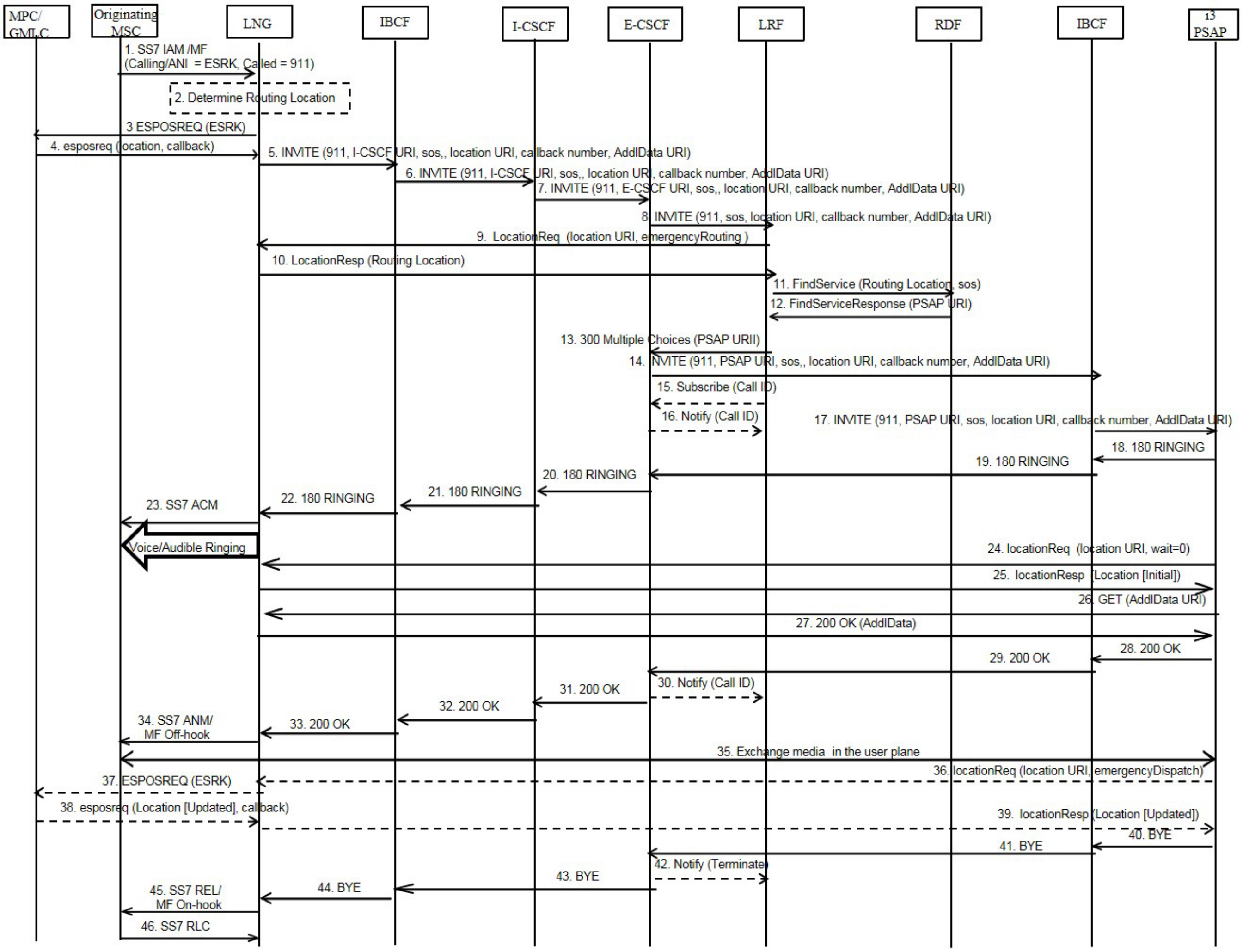

MPC/ GMLC
Originating MSC
LNG
IBCF
I-CSCF
E-CSCF
LRF
RDF
IBCF
i3 PSAP
1. SS7 IAM /MF (Calling/ANI = ESRK, Called = 911)
2. Determine Routing Location
3 ESPOSREQ (ESRK)
4. esposreq (location, callback)
5. INVITE (911, I-CSCF URI, sos,, location URI, callback number, AddlData URI)
6. INVITE (911, I-CSCF URI, sos,, location URI, callback number, AddlData URI)
7. INVITE (911, E-CSCF URI, sos,, location URI, callback number, AddlData URI)
8. INVITE (911, sos, location URI, callback number, AddlData URI)
9. LocationReq (location URI, emergencyRouting )
10. LocationResp (Routing Location)
11. FindService (Routing Location, sos)
12. FindServiceResponse (PSAP URI)
13. 300 Multiple Choices (PSAP URII)
14. INVITE (911, PSAP URI, sos,, location URI, callback number, AddlData URI)
15. Subscribe (Call ID)
16. Notify (Call ID)
17. INVITE (911, PSAP URI, sos, location URI, callback number, AddlData URI)
18. 180 RINGING
19. 180 RINGING
20. 180 RINGING
21. 180 RINGING
22. 180 RINGING
23. SS7 ACM
Voice/Audible Ringing
24. locationReq (location URI, wait=0)
25. locationResp (Location [Initial])
26. GET (AddlData URI)
27. 200 OK (AddlData)
28. 200 OK
29. 200 OK
30. Notify (Call ID)
31. 200 OK
32. 200 OK
33. 200 OK
34. SS7 ANM/ MF Off-hook
35. Exchange media in the user plane
36. locationReq (location URI, emergencyDispatch)
37. ESPOSREQ (ESRK)
38. esposreq (Location [Updated], callback)
39. locationResp (Location [Updated])
40. BYE
41. BYE
42. Notify (Terminate)
43. BYE
44. BYE
45. SS7 REL/ MF On-hook
46. SS7 RLC

**Figure 8.3: Delivery of Legacy Wireless Emergency Call Origination to i3 PSAP Using WCM**

**Step 1.** The originating MSC sends an emergency call origination from a legacy wireless caller to an i3 LNG over an MF or SS7-supported trunk group. The call setup signaling includes the ESRK (as the calling number) and the digits "911" (as the called number).

**Step 2.** The LNG accesses pre-provisioned data that maps the ESRK received in incoming signaling from the MSC to a routing location chosen so that it will route to the target PSAP associated with the ESRK (i.e., the Associated Location). The LNG uses the routing location to query an i3 ECRF to obtain the Route URI associated with the I-CSCF in the IMS-based NG9-1-1 Emergency Services Network (not shown).

**Step 3.** The LNG queries an MPC/GMLC in the legacy wireless originating network to obtain callback and initial caller location information for the call. In this example, the LNG uses the E2 protocol. Note that Steps 2 and 3 may be performed in parallel, depending on the implementation.

**Step 4.** The MPC/GMLC responds with the callback number and initial caller location, as well as non-location information (e.g., class of service).

**Step 5.** The LNG generates an outgoing SIP INVITE message, populating the callback number obtained from the MPC/GMLC in the From and PAI headers, “911” (expressed as a URI) in the To header, a service URN of urn:service:sos in the Request-URI and the I-CSCF URI obtained from the ECRF in the Route header. The outgoing SIP INVITE message also includes a Geolocation header that contains a location reference URI, and a Geolocation-Routing header set to “yes”. The LNG creates an Additional Data structure per NENA-STA-010.3 [Ref 27] and passes it forward “by-reference” by including a Call-Info header with a reference URI in the outgoing SIP INVITE message. The LNG forwards this SIP INVITE message to the (ingress) IBCF.

**Step 6.** The (ingress) IBCF forwards the SIP INVITE message to the I-CSCF.

**Step 7.** The I-CSCF forwards the SIP INVITE to the pre-configured E-CSCF.

**Step 8.** The E-CSCF forwards the SIP INVITE to the LRF.

**Step 9.** Since the SIP INVITE contains a LbyR, the LRF generates a de-reference request to the element identified in the location URI (i.e., the LNG) to obtain the routing location for the call. This example illustrates the use of HELD as the de-referencing protocol with a responseTime parameter value of “emergencyRouting”.

**Step 10.** The LNG responds to the de-reference request by returning the routing location obtained in Step 2.

**Step 11.** The LRF queries the RDF with the routing location received in Step 10 and the emergency service URN (urn:service:sos) received in the SIP INVITE message from the E-CSCF.

**Step 12.** The RDF returns a Route URI. In this example, the Route URI is associated with an i3 PSAP that is served by the IMS-based NG9-1-1 Emergency Services Network.

**Step 13.** The LRF redirects the call back to the E-CSCF, passing the Route (PSAP) URI obtained in Step 12.

**Step 14.** The E-CSCF generates an outgoing SIP INVITE message, using the information received from the LNG and the LRF, and forwards it to the (egress) IBCF. The SIP INVITE message contains the callback number received from the LNG in the From and P-Asserted-Identity headers, “911” (expressed as a URI) in the To header, the PSAP URI in the Route header, the sos service URN in the Request-URI, the location URI (LbyR) in the Geolocation header, a Geolocation-Routing header set to “yes”, and a Call-Info header that contains the Additional Data URI received from the LNG.

**Step 15.** (Optional) The LRF may subscribe to the state of the call.

**Step 16.** (Conditional on Step 15) The E-CSCF sends an initial notification of the state.

**Step 17.** The (egress) IBCF forwards the SIP INVITE to the i3 PSAP.

**Step 18.** An indication that the call taker is being alerted is returned by the i3 PSAP to the (egress) IBCF (using a SIP 180 RINGING message).

**Step 19.** The (egress) IBCF passes the SIP 180 RINGING message to the E-CSCF.

**Step 20.** The E-CSCF passes the SIP 180 RINGING message to the I-CSCF.

**Step 21.** The I-CSCF passes the SIP 180 RINGING message to the (ingress) IBCF.

**Step 22.** The (ingress) IBCF passes the SIP 180 RINGING message to the LNG.

**Step 23.** The LNG interworks the SIP 180 RINGING message to an SS7 ACM (if the call was delivered to it over an SS7-supported trunk group) and returns it to the originating MSC. The LNG also generates audible ringing toward the caller.

**Step 24.** In this example, the SIP INVITE contains a location URI, so the i3 PSAP queries the LNG (as identified in the location URI) for initial caller location (i.e., responseTime contains a wait timer value of "0").

**Step 25.** The LNG supplies the initial caller location information from Step 4 to the PSAP. The initial caller location information is displayed at the PSAP CPE.

**Step 26.** In this example, the SIP INVITE contains an Additional Data URI, so the i3 PSAP queries the LNG (as identified in the URI) for Additional Data using an HTTPS GET operation.

**Step 27.** The LNG provides the requested Additional Data in a 200 OK response.[14]

**Step 28.** When the PSAP answers the call, it returns a SIP 200 OK message to the (egress) IBCF.

**Step 29.** The (egress) IBCF passes the SIP 200 OK message to the E-CSCF.

**Step 30.** (Conditional on Step 15) The E-CSCF sends a notification to the LRF updating the call state.

**Step 31.** The E-CSCF passes the SIP 200 OK message to the I-CSCF.

**Step 32.** The I-CSCF passes the SIP 200 OK message to the (ingress) IBCF.

**Step 33.** The (ingress) IBCF passes the SIP 200 OK message to the LNG.

**Step 34.** The LNG maps the SIP 200 OK message to an SS7 ANM message or MF off-hook signal to the originating MSC.

**Step 35.** At this point a two-way connection is established between the caller and the PSAP.

**Step 36.** (Optional) The PSAP queries the LNG (as identified in the location URI) for updated (dispatch) location information (responseTime parameter = "emergencyDispatch" in this example).

**Step 37.** (Conditional on Step 36) The LNG queries the MPC/GMLC for updated (dispatch) location. (Note that the value of the responseTime parameter [emergencyDispatch or a specific time value] will be used by the LRF to determine whether to query the MPC/GMLC.)

**Step 38.** (Conditional on Step 37) The MPC/GMLC returns updated (dispatch) location information (and the callback number) to the LNG.

**Step 39.** (Conditional on Step 36) The LNG supplies updated (dispatch) location to the PSAP for display at the PSAP.

**Step 40.** At some point the call is terminated. In this call flow, the PSAP terminates the call and sends a SIP BYE message to the (egress) IBCF.

**Step 41.** The SIP BYE is passed from the (egress) IBCF to the E-CSCF.

**Step 42.** (Conditional on Step 15) The E-CSCF then notifies the LRF that the call has terminated.

**Step 43.** The E-CSCF passes the SIP BYE message to the (ingress) IBCF.

**Step 44.** The (ingress) IBCF passes the SIP BYE message to the LNG.

**Step 45.** The LNG maps the SIP BYE message to an SS7 REL message or an MF on-hook indication and sends it to the originating MSC.

**Step 46.** Upon receiving an SS7 REL message, the originating MSC sends an SS7 RLC message to the LNG.

[14] Note that Steps 24 through 27 can happen any time after Step 17, and that Steps 24 and 25 can be performed either before or after Steps 26 and 27.

### 8.2.2 Delivery of Legacy Wireless Emergency Call Origination to Legacy PSAP Using WCM

The call flow provided in Figure 8-4 illustrates a scenario where a legacy wireless emergency call is delivered by a legacy origination network via SS7 or MF trunks to an IMS-based NG9-1-1 Emergency Services Network using WCM. The call is delivered by the Mobile Switching Center (MSC) to an i3 LNG with an ESRK signaled as the SS7 Calling Party Number/MF ANI and the digits “911” as the called number. This call flow assumes that the LNG will determine the routing location for the call using local mappings based on the ESRK, and that it will also use the ESRK to query a Location Server (i.e., MPC/GMLC) in the legacy wireless network, using the E2 protocol, to obtain the caller location for the call. The LNG uses the routing location to query an ECRF (not shown) and then uses the URI provided in the ECRF response to route the call via an (ingress) IBCF to an I-CSCF in the IMS-based NG9-1-1 Emergency Services Network. The call is delivered to the IMS-based NG9-1-1 Emergency Services Network with a callback number, LbyR (i.e., a location URI), and Additional Data by reference (i.e., with a reference URI in a Call-Info header). The LRF uses the routing location and the sos service URN to query the RDF. This call flow assumes that the Route URI that is returned by the RDF is the URI associated with a legacy PSAP, and that the call is forwarded via an (egress) IBCF to an i3 LPG with the callback number, LbyR and Additional Data (by-reference) that was provided to the IMS-based NG9-1-1 Emergency Services Network by the LNG.

The call flow depicted in Figure 8-4 assumes that the LPG generates a pANI for the call and, based on per-PSAP provisioning, associates an appropriate Numbering Plan Digit (NPD) or ANI II value with the call (depending on whether the PSAP supports a Traditional MF interface or an Enhanced MF interface).

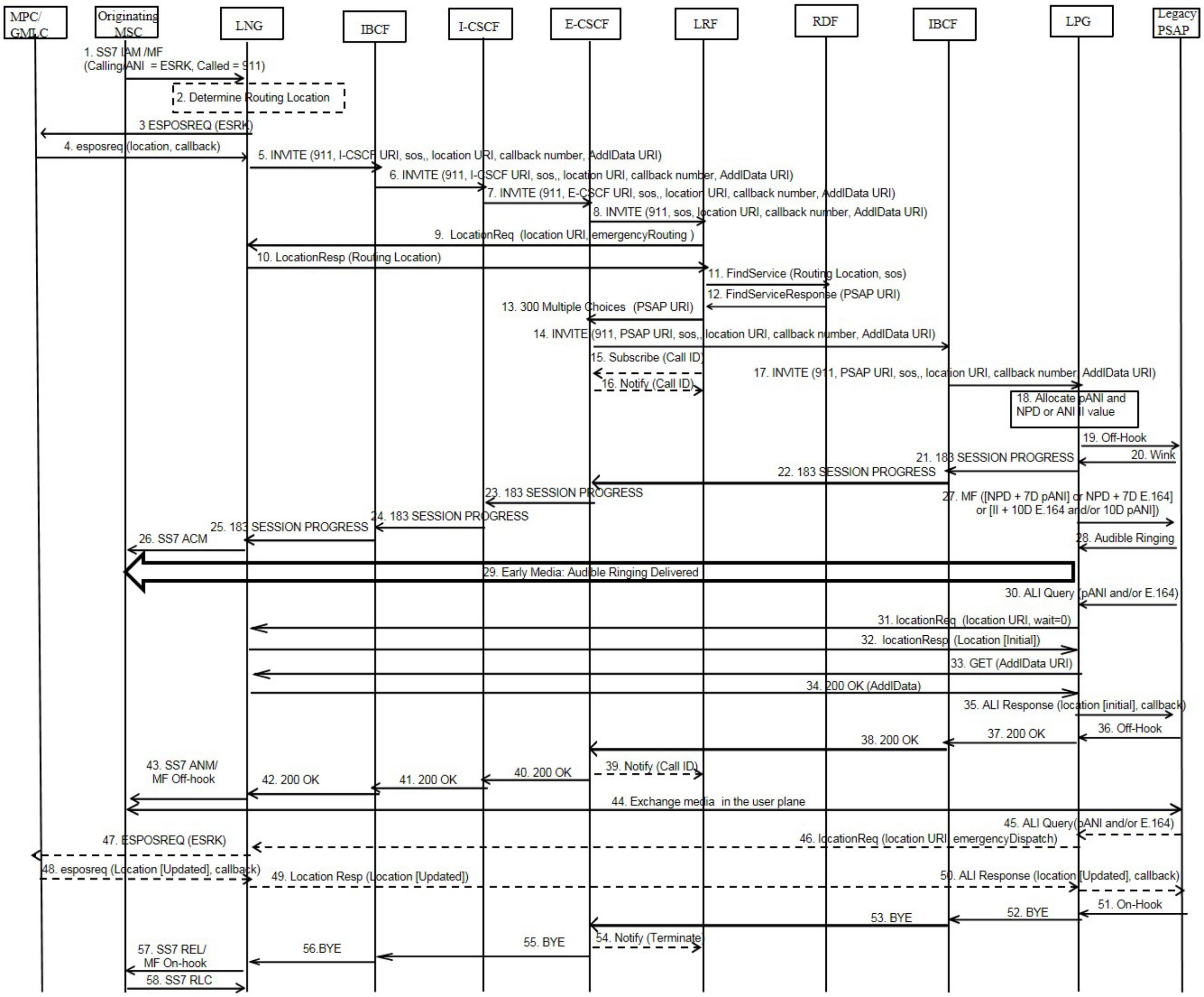

MPC/ GMLC
Originating MSC
LNG
IBCF
I-CSCF
E-CSCF
LRF
RDF
IBCF
LPG
Legacy PSAP
1. SS7 IAM /MF (Calling ANI = ESRK, Called = 911)
2. Determine Routing Location
3 ESPOSREQ (ESRK)
4. esposreq (location, callback)
5. INVITE (911, I-CSCF URI, sos,, location URI, callback number, AddlData URI)
6. INVITE (911, I-CSCF URI, sos,, location URI, callback number, AddlData URI)
7. INVITE (911, E-CSCF URI, sos,, location URI, callback number, AddlData URI)
8. INVITE (911, sos, location URI, callback number, AddlData URI)
9. LocationReq (location URI, emergencyRouting )
10. LocationResp (Routing Location)
11. FindService (Routing Location, sos)
12. FindServiceResponse (PSAP URI)
13. 300 Multiple Choices (PSAP URI)
14. INVITE (911, PSAP URI, sos,, location URI, callback number, AddlData URI)
15. Subscribe (Call ID)
16. Notify (Call ID)
17. INVITE (911, PSAP URI, sos,, location URI, callback number, AddlData URI)
18. Allocate pANI and NPD or ANI II value
19. Off-Hook
20. Wink
21. 183 SESSION PROGRESS
22. 183 SESSION PROGRESS
23. 183 SESSION PROGRESS
24. 183 SESSION PROGRESS
25. 183 SESSION PROGRESS
26. SS7 ACM
27. MF ([NPD + 7D pANI] or NPD + 7D E.164] or [II + 10D E.164 and/or 10D pANI])
28. Audible Ringing
29. Early Media: Audible Ringing Delivered
30. ALI Query (pANI and/or E.164)
31. locationReq (location URI, wait=0)
32. locationResp (Location [Initial])
33. GET (AddlData URI)
34. 200 OK (AddlData)
35. ALI Response (location [initial], callback)
36. Off-Hook
37. 200 OK
38. 200 OK
39. Notify (Call ID)
40. 200 OK
41. 200 OK
42. 200 OK
43. SS7 ANM/ MF Off-hook
44. Exchange media in the user plane
45. ALI Query(pANI and/or E.164)
46. locationReq (location URI, emergencyDispatch)
47. ESPOSREQ (ESRK)
48. esposreq (Location [Updated], callback)
49. Location Resp (Location [Updated])
50. ALI Response (location [Updated], callback)
51. On-Hook
52. BYE
53. BYE
54. Notify (Terminate)
55. BYE
56.BYE
57. SS7 REL/ MF On-hook
58. SS7 RLC

**Figure 8.4: Delivery of Legacy Wireless Emergency Call Origination to Legacy PSAP Using WCM**

**Step 1.** The originating MSC sends an emergency call origination from a legacy wireless caller to an i3 LNG over an MF or SS7-supported trunk group. The call setup signaling includes the ESRK (as the calling number) and the digits “911” (as the called number).

**Step 2.** The LNG accesses pre-provisioned data that maps the ESRK received in incoming signaling from the MSC to a routing location chosen so that it will route to the target PSAP associated with the ESRK (i.e., the Associated Location). The LNG uses the routing location to query an i3 ECRF to obtain the Route URI associated with the I-CSCF in the IMS-based NG9-1-1 Emergency Services Network (not shown).

**Step 3.** The LNG queries an MPC/GMLC in the legacy wireless originating network to obtain callback and initial caller location information for the call. In this example, the LNG uses the E2 protocol. Note that Steps 2 and 3 may be performed in parallel, depending on the implementation.

**Step 4.** The MPC/GMLC responds with the callback number and initial caller location, as well as non-location information (e.g., class of service).

**Step 5.** The LNG generates an outgoing SIP INVITE message, populating the callback number obtained from the MPC/GMLC in the From and PAI headers, “911” (expressed as a URI) in the To header, a service URN of urn:service:sos in the Request-URI, and the I-CSCF URI obtained from the ECRF in the Route header. The outgoing SIP INVITE message also includes a Geolocation header that contains a location reference URI, and a Geolocation-Routing header set to “yes”. The LNG creates an Additional Data structure per NENA-STA-010.3 [Ref 27] and passes it forward “by-reference” by including a Call-Info header with a reference URI in the outgoing SIP INVITE message. The LNG forwards this SIP INVITE message to the (ingress) IBCF.

**Step 6.** The (ingress) IBCF forwards the SIP INVITE message to the I-CSCF.

**Step 7.** The I-CSCF forwards the SIP INVITE to the pre-configured E-CSCF.

**Step 8.** The E-CSCF forwards the SIP INVITE to the LRF.

**Step 9.** Since the SIP INVITE contains a LbyR, the LRF generates a de-reference request to the element identified in the location URI (i.e., the LNG) to obtain the routing location for the call. This example illustrates the use of HELD as the de-referencing protocol, with a responseTime parameter value of “emergencyRouting”.

**Step 10.** The LNG responds to the de-reference request by returning the routing location obtained in Step 2.

**Step 11.** The LRF queries the RDF with the routing location received in Step 10 and the emergency service URN (urn:service:sos) received in the SIP INVITE message from the E-CSCF.

**Step 12.** The RDF returns a Route URI. In this example, the Route URI is associated with a legacy PSAP that is served by the IMS-based NG9-1-1 Emergency Services Network.

**Step 13.** The LRF redirects the call back to the E-CSCF, passing the Route (PSAP) URI.

**Step 14.** The E-CSCF generates an outgoing SIP INVITE message, using the information received from the LNG and the LRF, and forwards it to the (egress) IBCF. The SIP INVITE message contains the callback number received from the LNG in the From and P-Asserted Identity headers, “911” (expressed as a URI) in the To header, the PSAP URI in the Route header, the sos service URN in the Request-URI, the location URI (LbyR) in the Geolocation header, a Geolocation-Routing header set to “yes”, and a Call-Info header that contains the Additional Data URI received from the LNG.

**Step 15.** (Optional) The LRF may subscribe to the state of the call.

**Step 16.** (Conditional on Step 15) The E-CSCF sends an initial notification of the state.

**Step 17.** The (egress) IBCF forwards the SIP INVITE to the LPG.

**Step 18.** The LPG determines, based on provisioning, whether the PSAP associated with the received PSAP URI supports a Traditional MF or Enhanced MF interface. Depending on the type of interface supported by the PSAP, the LPG generates a pANI and assigns an appropriate NPD or ANI II value to the call, following the procedures specified in Clause 6.2.2 of NENA-STA-010.3 [Ref 27].

**Step 19.** The LPG generates an off-hook signal toward the legacy PSAP.

**Step 20.** The legacy PSAP returns a wink signal back to the LPG.

**Step 21.** The LPG generates a 183 Session Progress message and sends it to the (egress) IBCF.

**Step 22.** The (egress) IBCF passes the 193 Session Progress message to the E-CSCF.

**Step 23.** The E-CSCF passes the 183 Session Progress message to the I-CSCF.

**Step 24.** The I-CSCF passes the 183 Session Progress message to the (ingress) IBCF.

**Step 25.** The (ingress) IBCF passes the 183 Session Progress message to the LNG.

**Step 26.** The LNG maps the 183 Session Progress message to an SS7 ACM (assuming that the call was received by the LNG over an SS7-supported trunk group) and passes it to the originating MSC.

**Step 27.** The LPG delivers the call to the legacy PSAP, mapping the SIP signaling from the incoming INVITE message to the outgoing Traditional or Enhanced MF signaling sequences.

- For PSAPs that support a Traditional MF interface where delivery of callback information is preferred, the LPG will map the information received in the From/P-Asserted-Identity headers of the incoming SIP INVITE message, adding an appropriate NPD digit (i.e., the NPD + 7D E.164 number), to the MF ANI sequence KP + NPD + NXX XXXX + ST.
- For PSAPs that support a Traditional MF interface where delivery of location information is preferred, the LPG will populate the pANI it generated, along with an appropriate NPD digit (i.e., the NPD + 7D pANI) in the MF ANI sequence KP + NPD + NXX XXXX + ST.
- For PSAPs that support an Enhanced MF interface with 10-digit delivery where delivery of callback information is preferred, the LPG will map the information received in the P-Asserted-Identity header of the SIP INVITE message along with an appropriate II value (i.e., the II digits plus the 10D E.164 number) to the MF ANI sequence KP + II + NPA NXX XXXX + ST´.
- For PSAPs that support an Enhanced MF interface with 10-digit delivery where delivery of location information is preferred, the LPG will populate the pANI it generated along with an appropriate II value (i.e., the II digits plus the 10D pANI) in the MF ANI sequence KP + II + NPA NXX XXXX + ST´.
- For PSAPs that support an Enhanced MF interface with 20-digit delivery, the LPG will populate the pANI that it generated and the information received in the PAI (i.e., the E.164 number) along with an appropriate II value in the MF sequence KP + II + NPA NXX XXXX + ST + KP + NPA NXX XXXX + ST, where the first 10-digit number is mapped from the PAI and the second 10-digit number contain the pANI.

**Step 28.** Audible ringing is returned by the legacy PSAP to the LPG.

**Step 29.** Audible ringing is passed to the originating MSC/caller.

**Step 30.** The legacy PSAP sends a location query to the LPG using a NENA-defined ALI query protocol. The ALI query includes the 10-digit pANI and/or the 10-digit E.164 number received in Step 27. (Note that this can happen any time after Step 27.)

**Step 31.** Since, in this example, LbyR was delivered to the LPG in the SIP INVITE message, the LPG sends a de-reference request to the LNG (as identified in the location URI) for initial caller location (i.e., responseTime contains a wait timer value of "0").

**Step 32.** The LNG returns the initial caller location from Step 4 to the LPG in the de-reference response.

**Step 33.** In this example, the SIP INVITE received by the LPG contains an Additional Data URI, so the LPG queries the LNG (as identified in the URI) for Additional Data using an HTTPS GET operation.

**Step 34.** The LNG provides the requested Additional Data in a 200 OK response.[15]

**Step 35.** The LPG returns an ALI response to the legacy PSAP that includes initial caller location information, a callback number and other information (e.g., class of service), as appropriate for the interface.

**Step 36.** When the PSAP answers the call, it returns an off-hook signal to the LPG.

**Step 37.** In response to the off-hook signal, the LPG generates a SIP 200 OK message and passes it to the (egress) IBCF.

**Step 38.** The (egress) IBCF passes the SIP 200 OK message to the E-CSCF.

**Step 39.** The E-CSCF sends a notification to the LRF updating the call state.

**Step 40.** The E-CSCF passes the SIP 200 OK message to the I-CSCF.

[15] Note that Steps 31 through 34 can happen any time after Step 27, and that Steps 31 and 32 can be performed either before or after Steps 33 and 34.

**Step 41.** The I-CSCF passes the SIP 200 OK message to the (ingress) IBCF.

**Step 42.** The (ingress) IBCF passes the SIP 200 OK message to the LNG.

**Step 43.** The LNG maps the SIP 200 OK message to an SS7 ANM message or MF off-hook signal to the originating MSC.

**Step 44.** At this point a two-way connection is established between the caller and the PSAP.

**Step 45.** (Optional) The PSAP queries the LPG for updated (dispatch) location information.

**Step 46.** (Conditional on Step 45) The LPG sends a de-reference request to the LNG (as identified in the location URI) for updated (dispatch) location information (responseTime parameter = "emergencyDispatch" in this example).

**Step 47.** (Conditional on Step 46) The LNG queries the MPC/GMLC for updated (dispatch) location. (Note that the value of the responseTime parameter [emergencyDispatch or a specific time value] will be used by the LNG to determine whether to query the MPC/GMLC.)

**Step 48.** (Conditional on Step 47) The MPC/GMLC returns updated (dispatch) location information to the LNG.

**Step 49.** (Conditional on Step 46) The LNG returns the updated (dispatch) location from Step 48 to the LPG in the de-reference response.

**Step 50.** (Conditional on Step 45) The LRF supplies updated (dispatch) location to the PSAP for display at the PSAP.

**Step 51.** At some point the call is terminated. In this call flow, the PSAP terminates the call and sends an on-hook indication to the LPG.

**Step 52.** The LPG maps the on-hook indication to a SIP BYE message and sends the SIP BYE message to the (egress) IBCF.

**Step 53.** The (egress) IBCF passes the SIP BYE message to the E-CSCF.

**Step 54.** The E-CSCF then notifies the LRF that the call has terminated.

**Step 55.** The E-CSCF passes the SIP BYE message to the (ingress) IBCF.

**Step 56.** The (ingress) IBCF passes the SIP BYE message to the LNG.

**Step 57.** The LNG maps the SIP BYE message to an SS7 REL message or an MF on-hook indication, as appropriate, and sends it to the originating MSC.

**Step 58.** Upon receiving an SS7 REL message, the originating MSC sends an SS7 RLC message to the LNG.

### 8.2.3 Delivery of Legacy Wireless Emergency Call Origination to i3 PSAP using NCAS

The call flow provided in Figure 8-5 illustrates a scenario where a legacy wireless emergency call is delivered by a legacy origination network via SS7 or MF trunks to an IMS-based NG9-1-1 Emergency Services Network using NCAS. The call is delivered to the LNG with an ESRD/ESRK signaled in the SS7 Generic Digits Parameter (GDP) or as the MF called number, the callback number (in the form of an E.164 number) in the SS7 Calling Party Number parameter or as the MF ANI, and if the call is delivered via an SS7-supported trunk group, the digits "911" in the SS7 Called Party Number parameter. This call flow assumes that the LNG will determine the routing location for the call using local mappings based on the ESRD/ESRK received in incoming signaling from the MSC. It also assumes that the LNG will use the ESRD/ESRK and the E.164 number to query an MPC/GMLC in the legacy wireless network (using the E2 protocol) to obtain the caller location for the call. The LNG uses the routing location to query an ECRF (not shown) and then uses the URI provided in the ECRF response to route the call via an (ingress) IBCF to an I-CSCF in the IMS-based NG9-1-1 Emergency Services Network. The call is delivered to the IMS-based NG9-1-1 Emergency Services Network with the callback/E.164 number, LbyR (i.e., a location URI), and Additional Data by reference (i.e., with a reference URI in a Call-Info header). The LRF uses the routing location and the sos service URN to query the RDF. This call flow assumes that the Route URI that is returned by the RDF is the URI associated with an i3 PSAP. The LRF returns the Route URI to the E-CSCF and the call is delivered to the i3 PSAP with location (i.e., LbyR), the callback/E.164 number, and Additional Data (by reference).

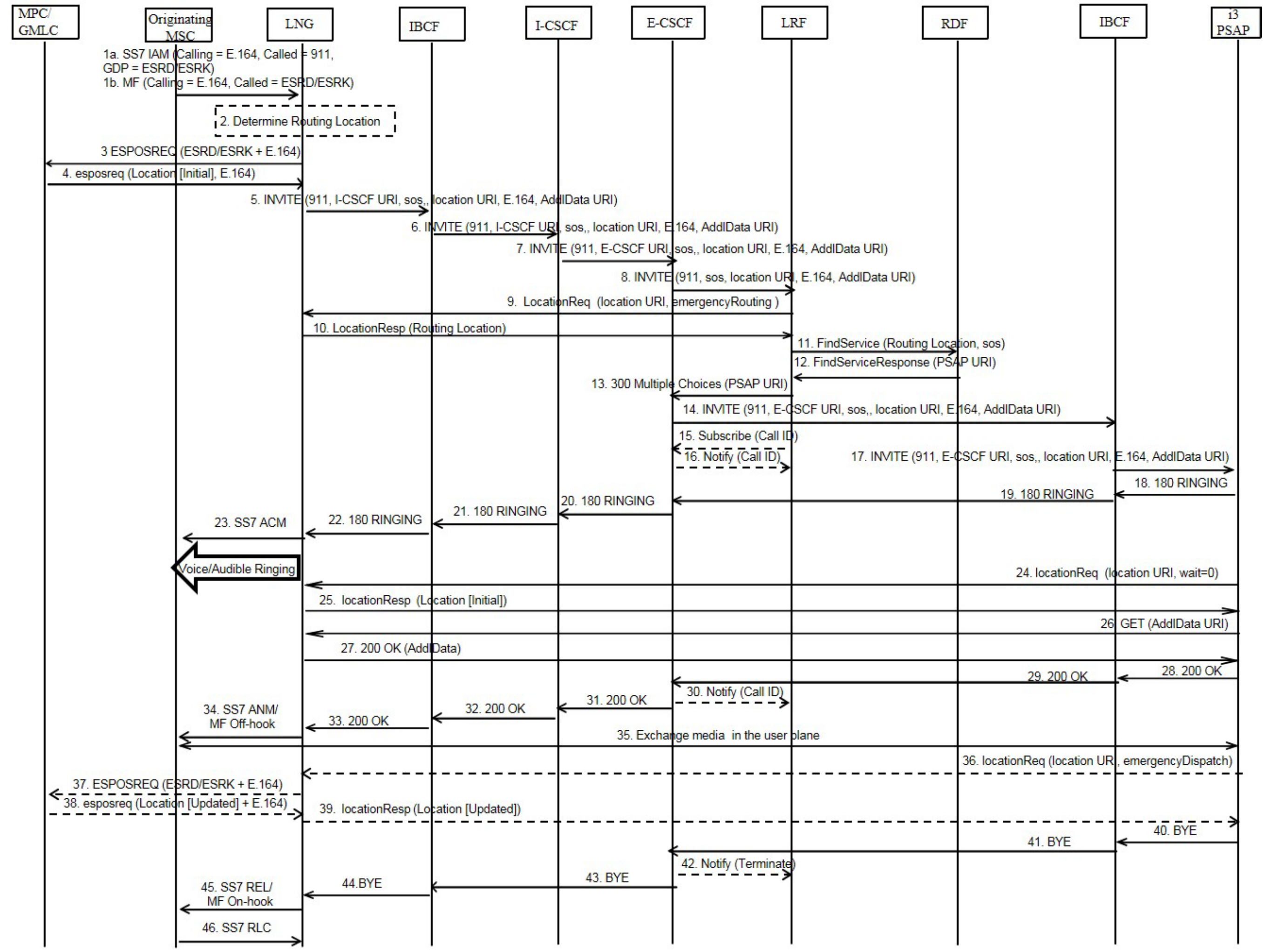

MPC/ GMLC
Originating MSC
LNG
IBCF
I-CSCF
E-CSCF
LRF
RDF
IBCF
i3 PSAP
1a. SS7 IAM (Calling = E.164, Called = 911, GDP = ESRD/ESRK)
1b. MF (Calling = E.164, Called = ESRD/ESRK)
2. Determine Routing Location
3 ESPOSREQ (ESRD/ESRK + E.164)
4. esposreq (Location [Initial], E.164)
5. INVITE (911, I-CSCF URI, sos,, location URI, E.164, AddlData URI)
6. INVITE (911, I-CSCF URI, sos,, location URI, E.164, AddlData URI)
7. INVITE (911, E-CSCF URI, sos,, location URI, E.164, AddlData URI)
8. INVITE (911, sos, location URI, E.164, AddlData URI)
9. LocationReq (location URI, emergencyRouting )
10. LocationResp (Routing Location)
11. FindService (Routing Location, sos)
12. FindServiceResponse (PSAP URI)
13. 300 Multiple Choices (PSAP URI)
14. INVITE (911, E-CSCF URI, sos,, location URI, E.164, AddlData URI)
15. Subscribe (Call ID)
16. Notify (Call ID)
17. INVITE (911, E-CSCF URI, sos,, location URI, E.164, AddlData URI)
18. 180 RINGING
19. 180 RINGING
20. 180 RINGING
21. 180 RINGING
22. 180 RINGING
23. SS7 ACM
Voice/Audible Ringing
24. locationReq (location URI, wait=0)
25. locationResp (Location [Initial])
26. GET (AddlData URI)
27. 200 OK (AddlData)
28. 200 OK
29. 200 OK
30. Notify (Call ID)
31. 200 OK
32. 200 OK
33. 200 OK
34. SS7 ANM/ MF Off-hook
35. Exchange media in the user plane
36. locationReq (location URI, emergencyDispatch)
37. ESPOSREQ (ESRD/ESRK + E.164)
38. esposreq (Location [Updated] + E.164)
39. locationResp (Location [Updated])
40. BYE
41. BYE
42. Notify (Terminate)
43. BYE
44.BYE
45. SS7 REL/ MF On-hook
46. SS7 RLC

**Figure 8.5: Delivery of Legacy Wireless Emergency Call Origination to i3 PSAP Using NCAS**

**Step 1.** The originating MSC sends an emergency call origination from a legacy wireless caller to the LNG over an MF or SS7-supported trunk group.

(a) If the call is delivered over an SS7 trunk group, the call setup signaling includes the calling (E.164) number sent in the Calling Party Number parameter, the ESRD/ESRK sent in the SS7 GDP, and the digits “911” in the SS7 Called Party Number parameter.

(b) If the call is delivered over an MF trunk group, the call setup signaling includes the ESRD/ESRK signaled as the called number, and the E.164 number signaled as the ANI.

**Step 2.** The LNG accesses pre-provisioned data that maps the ESRD/ESRK received in incoming signaling from the MSC to a routing location chosen so that it will route to the target PSAP associated with the ESRD/ESRK (i.e., the Associated Location). The LNG uses the routing location to query an i3 ECRF to obtain the Route URI associated with the I-CSCF in the IMS-based NG9-1-1 Emergency Services Network (not shown).

**Step 3.** The LNG queries an MPC/GMLC in the legacy wireless originating network (using the ESRD/ESRK and the E.164 number received in incoming signaling from the MSC) to obtain initial caller location information for the call. In this example, the LNG uses the E2 protocol. Note that Steps 2 and 3 may be performed in parallel, depending on the implementation.

**Step 4.** The MPC/GMLC responds with the callback number and initial caller location, as well as non-location information (e.g., class of service).

**Step 5.** The LNG generates an outgoing SIP INVITE message, populating the E.164 number received from the MSC in the From and PAI headers, “911” (expressed as a URI) in the To header, a service URN of urn:service:sos in the Request-URI and the I-CSCF URI obtained from the ECRF in the Route header. The outgoing SIP INVITE message also includes a Geolocation header that contains a location reference URI, and a Geolocation-Routing header set to “yes”. The LNG creates an Additional Data structure per NENA-STA-010.3 [Ref 27] and passes it forward “by-reference” by including a Call-Info header with a reference URI in the outgoing SIP INVITE message. The LNG forwards this SIP INVITE message to the (ingress) IBCF.

**Step 6.** The (ingress) IBCF forwards the SIP INVITE message to the I-CSCF.

**Step 7.** The I-CSCF forwards the SIP INVITE to the pre-configured E-CSCF.

**Step 8.** The E-CSCF forwards the SIP INVITE to the LRF.

**Step 9.** Since the SIP INVITE contains a LbyR, the LRF generates a de-reference request to the element identified in the location URI (i.e., the LNG) to obtain the routing location for the call. This example illustrates the use of HELD as the de-referencing protocol, with a responseTime parameter value of “emergencyRouting”.

**Step 10.** The LNG responds to the de-reference request by returning the routing location obtained in Step 2.

**Step 11.** The LRF queries the RDF with the routing location received in Step 10 and the emergency service URN (urn:service:sos) received in the SIP INVITE message from the E-CSCF.

**Step 12.** The RDF returns a Route URI. In this example, the Route URI is associated with an i3 PSAP that is served by the IMS-based NG9-1-1 Emergency Services Network.

**Step 13.** The LRF redirects the call back to the E-CSCF, passing the Route (PSAP) URI.

**Step 14.** The E-CSCF generates an outgoing SIP INVITE message, using the information received from the LNG and the LRF, and forwards it to the (egress) IBCF. The SIP INVITE message contains: the digits “911” (expressed as a URI) in the To header; the PSAP URI in the Route header; the sos service URN in the Request-URI; the E.164 number in the P-Asserted-Identity and From headers; the LbyR in the Geolocation header, a Geolocation-Routing header set to “yes”, and a pointer (i.e., reference URI) in the Call-Info header to the Additional Data structure created by the LNG.

**Step 15.** (Optional) The LRF may subscribe to the state of the call.

**Step 16.** (Conditional on Step 15) The E-CSCF sends an initial notification of the state.

**Step 17.** The (egress) IBCF forwards the SIP INVITE to the i3 PSAP.

**Step 18.** An indication that the call taker is being alerted is returned by the i3 PSAP to the (egress) IBCF (using a SIP 180 RINGING message).

**Step 19.** The IBCF passes the SIP 180 RINGING message to the E-CSCF.

**Step 20.** The E-CSCF passes the SIP 180 RINGING message to the I-CSCF.

**Step 21.** The I-CSCF passes the SIP 180 RINGING message to the (ingress) IBCF.

**Step 22.** The (ingress) IBCF passes the SIP 180 RINGING message to the LNG.

**Step 23.** The LNG interworks the SIP 180 RINGING message to an SS7 ACM (if the call was delivered to it over an SS7-supported trunk group) and returns it to the originating MSC. The LNG also generates audible ringing toward the caller.

**Step 24.** In this example, the SIP INVITE contains a location URI, so the i3 PSAP queries the LNG (as identified in the location URI) for initial caller location (i.e., responseTime contains a wait timer value of “0”).

**Step 25.** The LNG supplies the initial caller location information from Step 4 to the PSAP. The initial display location information is displayed at the PSAP CPE.

**Step 26.** In this example, the SIP INVITE contains an Additional Data URI, so the i3 PSAP queries the LNG (as identified in the URI) for Additional Data using an HTTPS GET operation.

**Step 27.** The LNG provides the requested Additional Data in a 200 OK response.[16]

**Step 28.** When the PSAP answers the call, it returns a SIP 200 OK message to the (egress) IBCF.

**Step 29.** The (egress) IBCF passes the SIP 200 OK message to the E-CSCF.

**Step 30.** The E-CSCF sends a notification to the LRF updating the call state.

**Step 31.** The E-CSCF passes the SIP 200 OK message to the I-CSCF.

**Step 32.** The I-CSCF passes the SIP 200 OK message to the (ingress) IBCF.

**Step 33.** The (ingress) IBCF passes the SIP 200 OK message to the LNG.

**Step 34.** The LNG maps the SIP 200 OK message to an SS7 ANM message or MF off-hook signal to the originating MSC.

**Step 35.** At this point a two-way connection is established between the caller and the PSAP.

**Step 36.** (Optional) The PSAP queries the LNG (as identified in the location URI) for updated (dispatch) location information (responseTime parameter = “emergencyDispatch” in this example).

**Step 37.** (Conditional on Step 36) The LNG queries the MPC/GMLC for updated (dispatch) location. (Note that the value of the responseTime parameter [emergencyDispatch or a specific time value] will be used by the LNG to determine whether to query the MPC/GMLC.)

**Step 38.** (Conditional on Step 37) The MPC/GMLC returns updated (dispatch) location information (and the callback number) to the LNG.

**Step 39.** (Conditional on Step 36) The LNG supplies updated (dispatch) location to the PSAP for display at the PSAP.

**Step 40.** At some point the call is terminated. In this call flow, the PSAP terminates the call and sends a SIP BYE message to the (egress) IBCF.

**Step 41.** The SIP BYE is passed from the (egress) IBCF to the E-CSCF.

**Step 42.** The E-CSCF then notifies the LRF that the call has terminated.

**Step 43.** The E-CSCF passes the SIP BYE message to the (ingress) IBCF.

**Step 44.** The (ingress) IBCF passes the SIP BYE message to the LNG.

**Step 45.** The LNG maps the SIP BYE message to an SS7 REL message or an MF on-hook indication and sends it to the originating MSC.

**Step 46.** Upon receiving an SS7 REL message, the originating MSC sends an SS7 RLC message to the LNG.

[16] Note that Steps 24 through 27 can happen any time after Step 17, and that Steps 24 and 25 can be performed either before or after Steps 26 and 27.

### 8.2.4 Delivery of Legacy Wireless Emergency Call Origination to Legacy PSAP using NCAS

The call flow provided in Figure 8-6 illustrates a scenario where a legacy wireless emergency call is delivered by a legacy origination network via SS7 or MF trunks to an IMS-based NG9-1-1 Emergency Services Network using NCAS. The call is delivered to the LNG with an ESRD/ESRK signaled in the SS7 Generic Digits Parameter (GDP) or as the MF called number, the callback number (in the form of an E.164 number) in the SS7 Calling Party Number parameter or as the MF ANI, and if the call is delivered via an SS7-supported trunk group, the digits “911” in the SS7 Called Party Number parameter. This call flow assumes that the LNG will determine the routing location for the call using local mappings based on the ESRD/ESRK received in incoming signaling from the MSC. It also assumes that the LNG will use the ESRD/ESRK and the E.164 number to query an MPC/GMLC in the legacy wireless network (using the E2 protocol) to obtain the caller location for the call. The LNG uses the routing location to query an ECRF (not shown) and then uses the URI provided in the ECRF response to route the call via an (ingress) IBCF to an I-CSCF in the IMS-based NG9-1-1 Emergency Services Network. The call is delivered to the IMS-based NG9-1-1 Emergency Services Network with the callback/E.164 number, LbyR (i.e., a location URI), and Additional Data by reference (i.e., with a reference URI in a Call-Info header). The LRF uses the routing location and the sos service URN to query the RDF. This call flow assumes that the Route URI that is returned by the RDF is the URI associated with a legacy PSAP, and that the call is forwarded via an (egress) IBCF to an i3 LPG with the callback/E.164 number, LbyR, and Additional Data (by-reference) that was provided to the IMS-based NG9-1-1 Emergency Services Network by the LNG.

The call flow depicted in Figure 8-6 assumes that the LPG generates a pANI for the call and, based on per-PSAP provisioning, associates an appropriate Numbering Plan Digit (NPD) or ANI II value with the call (depending on whether the PSAP supports a Traditional MF interface or an Enhanced MF interface).

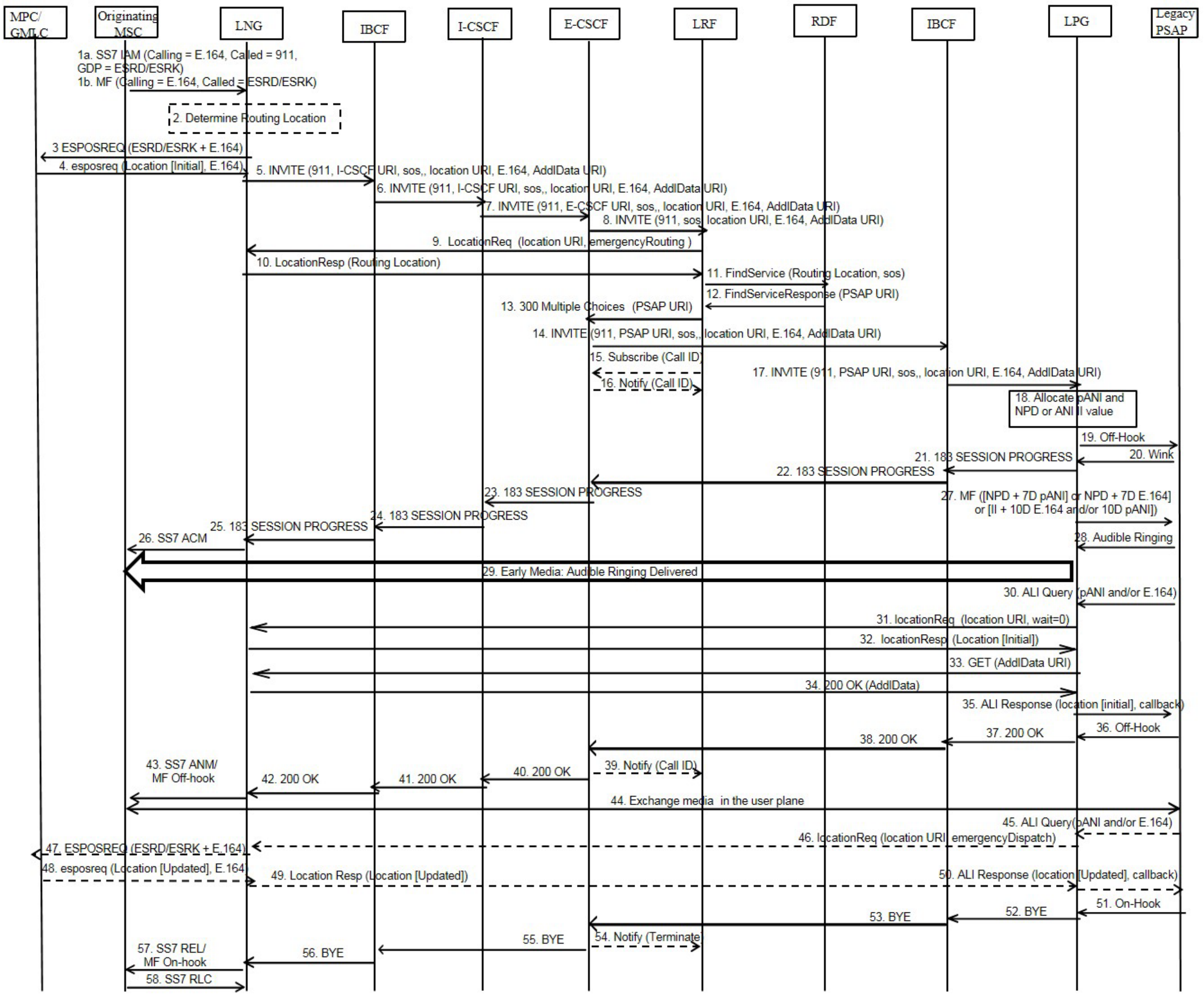

MPC/ GMLC
Originating MSC
LNG
IBCF
I-CSCF
E-CSCF
LRF
RDF
IBCF
LPG
Legacy PSAP
1a. SS7 IAM (Calling = E.164, Called = 911, GDP = ESRD/ESRK)
1b. MF (Calling = E.164, Called = ESRD/ESRK)
2. Determine Routing Location
3 ESPOSREQ (ESRD/ESRK + E.164)
4. esposreq (Location [Initial], E.164)
5. INVITE (911, I-CSCF URI, sos,, location URI, E.164, AddlData URI)
6. INVITE (911, I-CSCF URI, sos,, location URI, E.164, AddlData URI)
7. INVITE (911, E-CSCF URI, sos,, location URI, E.164, AddlData URI)
8. INVITE (911, sos, location URI, E.164, AddlData URI)
9. LocationReq (location URI, emergencyRouting )
10. LocationResp (Routing Location)
11. FindService (Routing Location, sos)
12. FindServiceResponse (PSAP URI)
13. 300 Multiple Choices (PSAP URI)
14. INVITE (911, PSAP URI, sos,, location URI, E.164, AddlData URI)
15. Subscribe (Call ID)
16. Notify (Call ID)
17. INVITE (911, PSAP URI, sos,, location URI, E.164, AddlData URI)
18. Allocate pANI and NPD or ANI II value
19. Off-Hook
20. Wink
21. 183 SESSION PROGRESS
22. 183 SESSION PROGRESS
23. 183 SESSION PROGRESS
24. 183 SESSION PROGRESS
25. 183 SESSION PROGRESS
26. SS7 ACM
27. MF ([NPD + 7D pANI] or NPD + 7D E.164] or [II + 10D E.164 and/or 10D pANI])
28. Audible Ringing
29. Early Media: Audible Ringing Delivered
30. ALI Query (pANI and/or E.164)
31. locationReq (location URI, wait=0)
32. locationResp (Location [Initial])
33. GET (AddlData URI)
34. 200 OK (AddlData)
35. ALI Response (location [initial], callback)
36. Off-Hook
37. 200 OK
38. 200 OK
39. Notify (Call ID)
40. 200 OK
41. 200 OK
42. 200 OK
43. SS7 ANM/ MF Off-hook
44. Exchange media in the user plane
45. ALI Query(pANI and/or E.164)
46. locationReq (location URI, emergencyDispatch)
47. ESPOSREQ (ESRD/ESRK + E.164)
48. esposreq (Location [Updated], E.164)
49. Location Resp (Location [Updated])
50. ALI Response (location [Updated], callback)
51. On-Hook
52. BYE
53. BYE
54. Notify (Terminate)
55. BYE
56. BYE
57. SS7 REL/ MF On-hook
58. SS7 RLC

**Figure 8.6: Delivery of Legacy Wireless Emergency Call Origination to Legacy PSAP Using NCAS**

**Step 1.** The originating MSC sends an emergency call origination from a legacy wireless caller to the LNG over an MF or SS7-supported trunk group.

(a) If the call is delivered over an SS7 trunk group, the call setup signaling includes the calling (E.164) number sent in the Calling Party Number parameter, the ESRD/ESRK sent in the SS7 GDP, and the digits "911" in the SS7 Called Party Number parameter.

(b) If the call is delivered over an MF trunk group, the call setup signaling includes the ESRD/ESRK signaled as the called number, and the E.164 number signaled as the ANI.

**Step 2.** The LNG accesses pre-provisioned data that maps the ESRD/ESRK received in incoming signaling from the MSC to a routing location chosen so that it will route to the target PSAP associated with the ESRD/ESRK (i.e., the Associated Location). The LNG uses the routing location to query an i3 ECRF to obtain the Route URI associated with the I-CSCF in the IMS-based NG9-1-1 Emergency Services Network (not shown).

**Step 3.** The LNG queries an MPC/GMLC in the legacy wireless originating network (using the ESRD/ESRK and the E.164 number received in incoming signaling from the MSC) to obtain initial display location information for the call. In this example, the LNG uses the E2 protocol. Note that Steps 2 and 3 may be performed in parallel, depending on the implementation.

**Step 4.** The MPC/GMLC responds with the callback number and initial display location, as well as non-location information (e.g., class of service).

**Step 5.** LNG generates an outgoing SIP INVITE message, populating the E.164 number received from the MSC in the From and PAI headers, “911” (expressed as a URI) in the To header, a service URN of urn:service:sos in the Request-URI, and the I-CSCF URI obtained from the ECRF in the Route header. The outgoing SIP INVITE message also includes a Geolocation header that contains a location reference URI, and a Geolocation-Routing header set to “yes”. The LNG creates an Additional Data structure per NENA-STA-010.3 [Ref 27] and passes it forward “by-reference” by including a Call-Info header with a reference URI in the outgoing SIP INVITE message. The LNG forwards this SIP INVITE message to the (ingress) IBCF.

**Step 6.** The (ingress) IBCF forwards the SIP INVITE message to the I-CSCF.

**Step 7.** The I-CSCF forwards the SIP INVITE to the pre-configured E-CSCF.

**Step 8.** The E-CSCF forwards the SIP INVITE to the LRF.

**Step 9.** Since the SIP INVITE contains a LbyR, the LRF generates a de-reference request to the element identified in the location URI (i.e., the LNG) to obtain the routing location for the call. This example illustrates the use of HELD as the de-referencing protocol, with a responseTime parameter value of “emergencyRouting”.

**Step 10.** The LNG responds to the de-reference request by returning the routing location obtained in Step 2.

**Step 11.** The LRF queries the RDF with the routing location received in Step 10 and the emergency service URN (urn:service:sos) received in the SIP INVITE message from the E-CSCF.

**Step 12.** The RDF returns a Route URI. In this example, the Route URI is associated with a legacy PSAP that is served by the IMS-based NG9-1-1 Emergency Services Network.

**Step 13.** The LRF redirects the call back to the E-CSCF, passing the Route (PSAP) URI.

**Step 14.** The E-CSCF generates an outgoing SIP INVITE message, using the information received from the LNG and the LRF, and forwards it to the (egress) IBCF. The SIP INVITE message contains “911” (expressed as a URI) in the To header; the PSAP URI in the Route header; the sos service URN in the Request-URI; the E.164 number in the P-Asserted-Identity and From headers; the LbyR in the Geolocation header, a Geolocation-Routing header set to “yes”, and a pointer (i.e., reference URI) in the Call-Info header to the Additional Data structure created by the LNG.

**Step 15.** (Optional) The LRF may subscribe to the state of the call.

**Step 16.** (Conditional on Step 15) The E-CSCF sends an initial notification of the state.

**Step 17.** The (egress) IBCF forwards the SIP INVITE to the LPG.

**Step 18.** The LPG determines, based on provisioning, whether the PSAP associated with the received PSAP URI supports a Traditional MF or Enhanced MF interface. Depending on the type of interface supported by the PSAP, the LPG may generate a pANI and will assign an appropriate NPD or ANI II value to the call, following the procedures specified in Clause 6.2.2 of NENA-STA-010.3 [Ref 27].

**Step 19.** The LPG generates an off-hook signal toward the legacy PSAP.

**Step 20.** The legacy PSAP returns a wink signal back to the LPG.

**Step 21.** The LPG generates a 183 Session Progress message and sends it to the (egress) IBCF.

**Step 22.** The (egress) IBCF passes the 183 Session Progress message to the E-CSCF.

**Step 23.** The E-CSCF passes the 183 Session Progress message to the I-CSCF.

**Step 24.** The I-CSCF passes the 183 Session Progress message to the (ingress) IBCF.

**Step 25.** The (ingress) IBCF passes the 183 Session Progress message to the LNG.

**Step 26.** The LNG maps the 183 Session Progress message to an SS7 ACM (assuming that the call was received by the LNG over an SS7-supported trunk group) and passes it to the originating MSC.

**Step 27.** The LPG delivers the call to the legacy PSAP, mapping the SIP signaling from the incoming INVITE message to the outgoing Traditional or Enhanced MF signaling sequences.

- For PSAPs that support a Traditional MF interface where delivery of callback information is preferred, the LPG will map the information received in the From/P-Asserted-Identity headers of the incoming SIP INVITE message, adding an appropriate NPD digit (i.e., the NPD + 7D E.164 number), to the MF ANI sequence KP + NPD + NXX XXXX + ST.
- For PSAPs that support a Traditional MF interface where delivery of location information is preferred, the LPG will populate the pANI it generated, along with an appropriate NPD digit (i.e., the NPD + 7D pANI) in the MF ANI sequence KP + NPD + NXX XXXX + ST.
- For PSAPs that support an Enhanced MF interface with 10-digit delivery where delivery of callback information is preferred, the LPG will map the information received in the P-Asserted-Identity header of the SIP INVITE message along with an appropriate II value (i.e., the II digits plus the 10D E.164 number) to the MF ANI sequence KP + II + NPA NXX XXXX + ST´.
- For PSAPs that support an Enhanced MF interface with 10-digit delivery where delivery of location information is preferred, the LPG will populate the pANI it generated along with an appropriate II value (i.e., the II digits plus the 10D pANI) in the MF ANI sequence KP + II + NPA NXX XXXX + ST´.
- For PSAPs that support an Enhanced MF interface with 20-digit delivery, the LPG will populate the pANI that it generated and the information received in the PAI (i.e., the E.164 number) along with an appropriate II value in the MF sequence KP + II + NPA NXX XXXX + ST + KP + NPA NXX XXXX + ST, where the first 10-digit number is mapped from the PAI and the second 10-digit number contain the pANI.

**Step 28.** Audible ringing is returned by the legacy PSAP to the LPG.

**Step 29.** Audible ringing is passed to the originating MSC/caller.

**Step 30.** The legacy PSAP sends a location query to the LPG using a NENA-defined ALI query protocol. The ALI query includes the 10-digit pANI and/or 10-digit E.164 number received in Step 27. (Note that this can happen any time after Step 27.)

**Step 31.** Since, in this example, LbyR was delivered to the LPG in the SIP INVITE message, the LPG sends a de-reference request to the LNG (as identified in the location URI) for initial display location (i.e., responseTime contains a wait timer value of "0").

**Step 32.** The LNG returns the initial display location from Step 4 to the LPG in the de-reference response.

**Step 33.** In this example, the SIP INVITE received by the LPG contains an Additional Data URI, so the LPG queries the LNG (as identified in the URI) for Additional Data using an HTTPS GET operation.

**Step 34.** The LNG provides the requested Additional Data in a 200 OK response.[17]

**Step 35.** The LPG returns an ALI response to the legacy PSAP that includes initial display location information, a callback number and other information (e.g., class of service), as appropriate for the interface.

**Step 36.** When the PSAP answers the call, it returns an off-hook signal to the LPG.

[17] Note that Steps 31 through 34 can happen any time after Step 27, and that Steps 31 and 32 can be performed either before or after Steps 33 and 34.

**Step 37.** In response to the off-hook signal, the LPG generates a SIP 200 OK message and passes it to the (egress) IBCF.

**Step 38.** The (egress) IBCF passes the SIP 200 OK message to the E-CSCF.

**Step 39.** The E-CSCF sends a notification to the LRF updating the call state.

**Step 40.** The E-CSCF passes the SIP 200 OK message to the I-CSCF.

**Step 41.** The I-CSCF passes the SIP 200 OK message to the (ingress) IBCF.

**Step 42.** The (ingress) IBCF passes the SIP 200 OK message to the LNG.

**Step 43.** The LNG maps the SIP 200 OK message to an SS7 ANM message or MF off-hook signal to the originating MSC.

**Step 44.** At this point a two-way connection is established between the caller and the PSAP.

**Step 45.** (Optional) The PSAP queries the LPG for updated (dispatch) location information.

**Step 46.** (Conditional on Step 45) The LPG sends a de-reference request to the LNG (as identified in the location URI) for updated (dispatch) location information (responseTime parameter = "emergencyDispatch" in this example).

**Step 47.** (Conditional on Step 46) The LNG queries the MPC/GMLC for updated (dispatch) location. (Note that the value of the responseTime parameter [emergencyDispatch or a specific time value] will be used by the LNG to determine whether to query the MPC/GMLC.)

**Step 48.** (Conditional on Step 47) The MPC/GMLC returns updated (dispatch) location information to the LNG.

**Step 49.** (Conditional on Step 46) The LNG returns the updated (dispatch) location from Step 48 to the LPG in the de-reference response.

**Step 50.** (Conditional on Step 45) The LPG supplies updated (dispatch) location to the PSAP for display at the PSAP.

**Step 51.** At some point the call is terminated. In this call flow, the PSAP terminates the call and sends an on-hook indication to the LPG.

**Step 52.** The LPG maps the on-hook indication to a SIP BYE message and sends the SIP BYE message to the (egress) IBCF.

**Step 53.** The (egress) IBCF passes the SIP BYE message to the E-CSCF.

**Step 54.** The E-CSCF then notifies the LRF that the call has terminated.

**Step 55.** The E-CSCF passes the SIP BYE message to the (ingress) IBCF.

**Step 56.** The (ingress) IBCF passes the SIP BYE message to the LNG.

**Step 57.** The LNG maps the SIP BYE message to an SS7 REL message or an MF on-hook indication, as appropriate, and sends it to the originating MSC.

**Step 58.** Upon receiving an SS7 REL message, the originating MSC sends an SS7 RLC message to the LNG.

## *8.3 IMS Originating Network to i3 and Legacy PSAPs – LbyV*

### 8.3.1 Delivery of Emergency Call Origination from IMS Origination Network to i3 PSAP with LbyV

The call flow provided in Figure 8-7 illustrates a scenario where an emergency call is delivered by an IMS origination network to an IMS-based NG9-1-1 Emergency Services Network with LbyV. The call is delivered to an IBCF on the ingress side of the IMS-based NG9-1-1 Emergency Services Network. The SIP INVITE message signaled by the IMS originating network includes a Route header that contains the URI of an I-CSCF in the IMS-based NG9-1-1 Emergency Services Network, an emergency services service URN (urn:service:sos) in the Request-URI, callback information in the P-Asserted-Identity header, and LbyV and Additional Data "by value" in the message body. (A Geolocation header that contains a Content-ID (cid) pointing to the PIDF-LO in the message body, a Geolocation-Routing header set to "yes", a Call-Info header that contains a cid pointing to the Additional Data in the message body, and other SIP headers will also be included in the SIP INVITE message, but are not specifically illustrated in Figure 8-7.) This call flow assumes that the I-CSCF forwards the SIP INVITE message to the E-CSCF. The E-CSCF forwards the SIP INVITE message to the LRF. The LRF uses the LbyV to query the RDF. In this example call flow, the Route URI that is returned by the RDF is associated with an i3 PSAP. This call flow assumes that the call is delivered to the i3 PSAP with LbyV and Additional Data "by value". (See Clause 8.12.1 for a call flow illustrating the application of SHAKEN caller identity authentication/verification and RPH signing/verification to an emergency call origination from an IMS origination network to an i3 PSAP.)

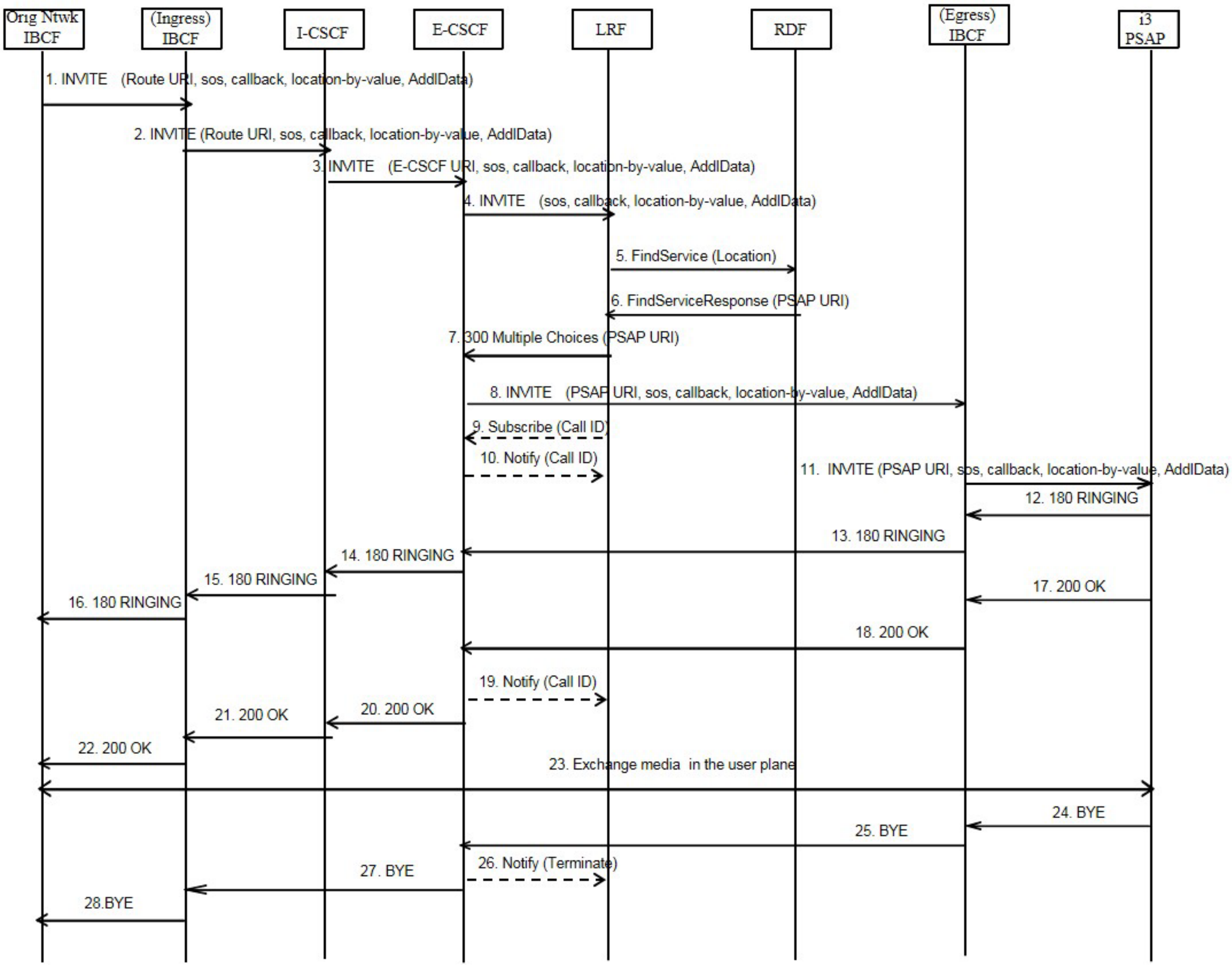

Orig Ntwk IBCF
(Ingress) IBCF
I-CSCF
E-CSCF
LRF
RDF
(Egress) IBCF
i3 PSAP
1. INVITE (Route URI, sos, callback, location-by-value, AddlData)
2. INVITE (Route URI, sos, callback, location-by-value, AddlData)
3. INVITE (E-CSCF URI, sos, callback, location-by-value, AddlData)
4. INVITE (sos, callback, location-by-value, AddlData)
5. FindService (Location)
6. FindServiceResponse (PSAP URI)
7. 300 Multiple Choices (PSAP URI)
8. INVITE (PSAP URI, sos, callback, location-by-value, AddlData)
9. Subscribe (Call ID)
10. Notify (Call ID)
11. INVITE (PSAP URI, sos, callback, location-by-value, AddlData)
12. 180 RINGING
13. 180 RINGING
14. 180 RINGING
15. 180 RINGING
16. 180 RINGING
17. 200 OK
18. 200 OK
19. Notify (Call ID)
20. 200 OK
21. 200 OK
22. 200 OK
23. Exchange media in the user plane
24. BYE
25. BYE
26. Notify (Terminate)
27. BYE
28.BYE

**Figure 8.7: Delivery of IMS Emergency Call Origination to i3 PSAP with LbyV**

**Step 1.** The IBCF in the IMS originating network sends an emergency call origination to an (ingress) IBCF in the IMS-based NG9-1-1 Emergency Services Network. The SIP INVITE message includes a Route header that contains the I-CSCF URI, an emergency services service URN (urn:service:sos), callback information, LbyV, and Additional Data (by value).

**Step 2.** The (ingress) IBCF forwards the received INVITE message to the I-CSCF.

**Step 3.** The I-CSCF forwards the SIP INVITE to the pre-configured E-CSCF. The SIP INVITE message sent to the E-CSCF by the I-CSCF contains the E-CSCF URI in the Route header, and includes the callback information, “sos” service URN, LbyV, and Additional Data (by value), as received in the incoming SIP INVITE message.

**Step 4.** The E-CSCF forwards the SIP INVITE to the LRF.

**Step 5.** LRF queries the RDF using the location information received in the body of the received SIP INVITE message and the emergency service URN (urn:service:sos).

**Step 6.** The RDF returns a Route URI. In this example, the Route URI is associated with an i3 PSAP that is served by the IMS-based NG9-1-1 Emergency Services Network.

**Step 7.** The LRF redirects the call back to the E-CSCF, passing the Route (PSAP) URI.

**Step 8.** The E-CSCF generates an outgoing SIP INVITE message, using the information received from the LRF as well as information received in the initial SIP INVITE message, and forwards it to the (egress) IBCF. The SIP INVITE message contains the PSAP URI in the Route header, the sos service URN in the Request-URI, the callback information in the From and P-Asserted-Identity headers, the LbyV in the body (along with a cid in the Geolocation header and a Geolocation-Routing header set to “yes”), and Additional Data (by value) in the body (along with a cid in the Call-Info header).

**Step 9.** (Optional) The LRF may subscribe to the state of the call.

**Step 10.** (Conditional on Step 9) The E-CSCF sends an initial notification of the call state.

**Step 11.** The (egress) IBCF forwards the SIP INVITE to the i3 PSAP with the callback information, the LbyV, and the Additional Data received in the initial SIP INVITE message from the IMS originating network.

**Step 12.** An indication that the call taker is being alerted is returned by the i3 PSAP to the (egress) IBCF (using a SIP 180 RINGING message).

**Step 13.** The (egress) IBCF passes the SIP 180 RINGING message to the E-CSCF.

**Step 14.** The E-CSCF passes the SIP 180 RINGING message to the I-CSCF.

**Step 15.** The I-CSCF passes the SIP 180 RINGING message to the (ingress) IBCF.

**Step 16.** The (ingress) IBCF passes the SIP 180 RINGING message to the originating network via the originating network IBCF.

**Step 17.** When the PSAP answers the call, it returns a SIP 200 OK message to the (egress) IBCF.

**Step 18.** The (egress) IBCF passes the SIP 200 OK message to the E-CSCF.

**Step 19.** (Conditional on Step 9) The E-CSCF sends a notification to the LRF updating the call state.

**Step 20.** The E-CSCF passes the SIP 200 OK message to the I-CSCF.

**Step 21.** The I-CSCF passes the SIP 200 OK message to the (ingress) IBCF.

**Step 22.** The (ingress) IBCF passes the SIP 200 OK message to the originating network via the originating network IBCF.

**Step 23.** At this point a two-way connection is established between the caller and the PSAP.

**Step 24.** At some point the call is terminated. In this call flow, the PSAP terminates the call and sends a SIP BYE message to the (egress) IBCF.

**Step 25.** The SIP BYE is passed from the (egress) IBCF to the E-CSCF.

**Step 26.** (Conditional on Step 9) The E-CSCF then notifies the LRF that the call has terminated.

**Step 27.** The E-CSCF passes the SIP BYE message to the (ingress) IBCF.

**Step 28.** The (ingress) IBCF passes the SIP BYE message to the originating network via the originating network IBCF.

### 8.3.2 Delivery of Emergency Call Origination from IMS Origination Network to Legacy PSAP with LbyV

The call flow provided in Figure 8-8 illustrates a scenario where an emergency call is delivered by an IMS origination network to an IMS-based NG9-1-1 Emergency Services Network with LbyV. The call is delivered to an IBCF on the ingress side of the IMS-based NG9-1-1 Emergency Services Network. The SIP INVITE message signaled by the IMS originating network includes a Route header that contains the URI of an I-CSCF in the IMS-based NG9-1-1 Emergency Services Network, an emergency services service URN (urn:service:sos) in the Request-URI, callback information in the P-Asserted-Identity header, and LbyV and Additional Data (by value) in the message body. (A Geolocation header that contains a cid pointing to the PIDF-LO in the message body, a Geolocation-Routing header set to “yes”, a Call-Info header that contains a cid pointing to the Additional Data in the message body, and other

SIP headers will also be included in the SIP INVITE message, but are not specifically illustrated in Figure 8-8.) This call flow assumes that the I-CSCF forwards the SIP INVITE message to the E-CSCF. The E-CSCF forwards the SIP INVITE message to the LRF. The LRF uses the LbyV to query the RDF. In this example call flow, the Route URI that is returned by the RDF is associated with a legacy PSAP, and the call is forwarded via an (egress) IBCF to an i3 LPG with the LbyV and Additional Data (by value) that was provided to the IMS-based NG9-1-1 Emergency Services Network by the IMS originating network. The call flow depicted in Figure 8-8 assumes that the LPG generates a 7/10-digit pANI for the call and, based on per-PSAP provisioning, associates an appropriate Numbering Plan Digit (NPD) or ANI II value with the call (depending on whether the PSAP supports a Traditional MF interface or an Enhanced MF interface).

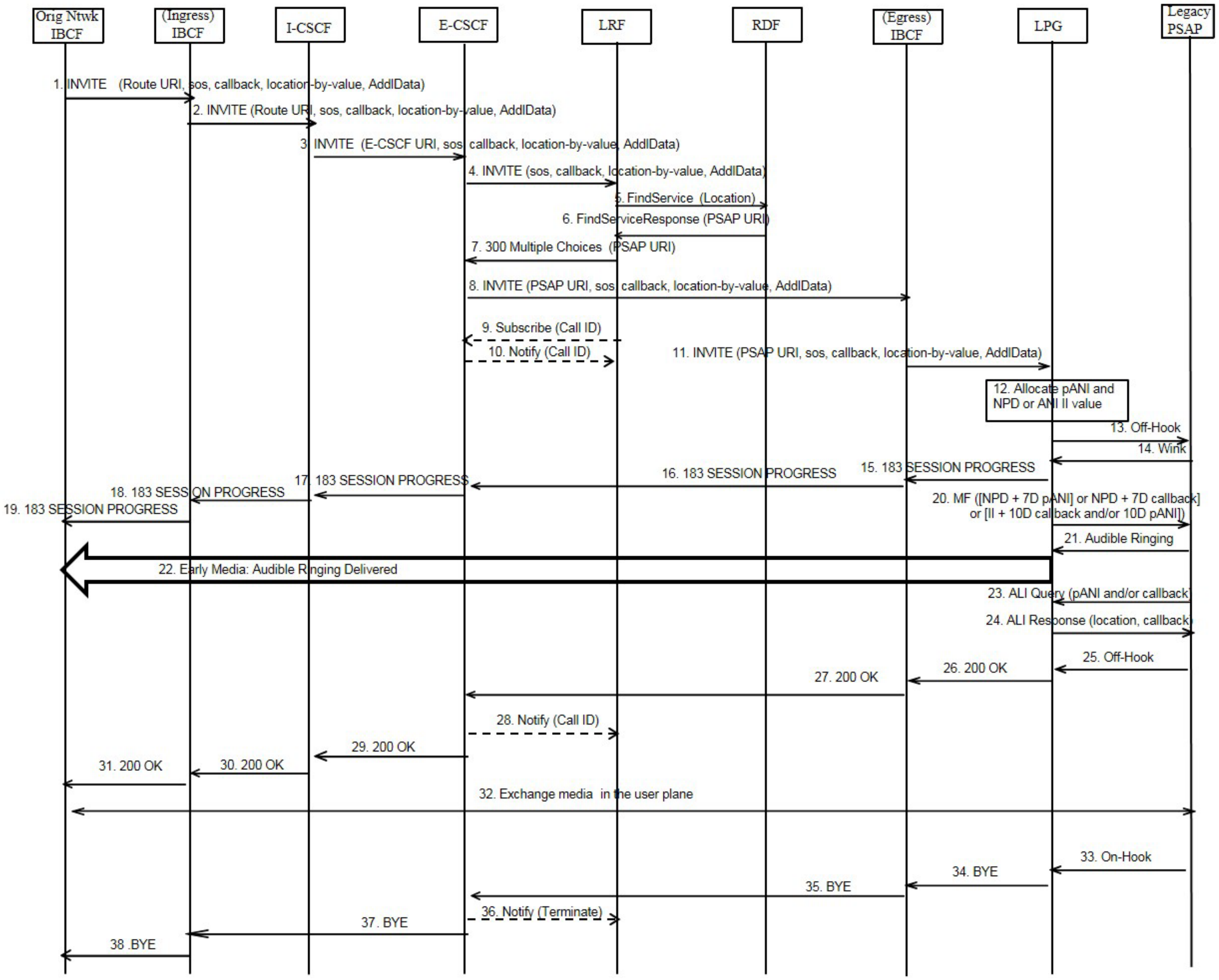

Orig Ntwk IBCF
(Ingress) IBCF
I-CSCF
E-CSCF
LRF
RDF
(Egress) IBCF
LPG
Legacy PSAP
1. INVITE (Route URI, sos, callback, location-by-value, AddlData)
2. INVITE (Route URI, sos, callback, location-by-value, AddlData)
3. INVITE (E-CSCF URI, sos, callback, location-by-value, AddlData)
4. INVITE (sos, callback, location-by-value, AddlData)
5. FindService (Location)
6. FindServiceResponse (PSAP URI)
7. 300 Multiple Choices (PSAP URI)
8. INVITE (PSAP URI, sos, callback, location-by-value, AddlData)
9. Subscribe (Call ID)
10. Notify (Call ID)
11. INVITE (PSAP URI, sos, callback, location-by-value, AddlData)
12. Allocate pANI and NPD or ANI II value
13. Off-Hook
14. Wink
15. 183 SESSION PROGRESS
16. 183 SESSION PROGRESS
17. 183 SESSION PROGRESS
18. 183 SESSION PROGRESS
19. 183 SESSION PROGRESS
20. MF ([NPD + 7D pANI] or NPD + 7D callback] or [II + 10D callback and/or 10D pANI])
21. Audible Ringing
22. Early Media: Audible Ringing Delivered
23. ALI Query (pANI and/or callback)
24. ALI Response (location, callback)
25. Off-Hook
26. 200 OK
27. 200 OK
28. Notify (Call ID)
29. 200 OK
30. 200 OK
31. 200 OK
32. Exchange media in the user plane
33. On-Hook
34. BYE
35. BYE
36. Notify (Terminate)
37. BYE
38 .BYE

**Figure 8.8: Delivery of IMS Emergency Call Origination to Legacy PSAP with LbyV**

**Step 1.** The IBCF in the IMS originating network sends an emergency call origination to an (ingress) IBCF in the IMS-based NG9-1-1 Emergency Services Network. The SIP INVITE message includes a Route header that contains the I-CSCF URI, an emergency services service URN (urn:service:sos), callback information, LbyV, and Additional Data (by value).

**Step 2.** The (ingress) IBCF forwards the received INVITE message to the I-CSCF.

**Step 3.** The I-CSCF forwards the SIP INVITE to the pre-configured E-CSCF. The SIP INVITE message sent to the E-CSCF by the I-CSCF contains the E-CSCF URI in the Route header, and includes the callback information, "sos" service URN, LbyV, and Additional Data (by value), as received in the incoming SIP INVITE message.

**Step 4.** The E-CSCF forwards the SIP INVITE to the LRF.

**Step 5.** LRF queries the RDF using the location information received in the body of the received SIP INVITE message and the emergency service URN (urn:service:sos).

**Step 6.** The RDF returns a Route URI. In this example, the Route URI is associated with a legacy PSAP that is served by the IMS-based NG9-1-1 Emergency Services Network.

**Step 7.** The LRF redirects the call back to the E-CSCF, passing the Route (PSAP) URI.

**Step 8.** The E-CSCF generates an outgoing SIP INVITE message, using the information received from the LRF, as well as information received in the initial SIP INVITE message, and forwards it to the (egress) IBCF. The SIP INVITE message includes the PSAP URI in the Route header; the sos service URN in the Request-URI; the callback number in the P-Asserted-Identity and From headers; a cid in the Geolocation header; a Geolocation-Routing header set to "yes"; a cid in the Call-Info header; and LbyV and Additional Data (by value) in the message body.

**Step 9.** (Optional) The LRF may subscribe to the state of the call.

**Step 10.** (Conditional on Step 9) The E-CSCF sends an initial notification of the call state.

**Step 11.** The (egress) IBCF forwards the SIP INVITE to the LPG.

**Step 12.** The LPG determines, based on provisioning, whether the PSAP associated with the received PSAP URI supports a Traditional MF or Enhanced MF interface. Depending on the type of interface supported by the PSAP, the LPG may generate a pANI[18] and will assign an appropriate NPD or ANI II value to the call, following the procedures specified in Clause 6.2.2 of NENA-STA-010.3 [Ref 27].

**Step 13.** The LPG generates an off-hook signal toward the legacy PSAP.

**Step 14.** The legacy PSAP returns a wink signal back to the LPG.

**Step 15.** The LPG generates a 183 Session Progress message and sends it to the (egress) IBCF.

**Step 16.** The (egress) IBCF passes the 183 Session Progress message to the E-CSCF.

**Step 17.** The E-CSCF passes the 183 Session Progress message to the I-CSCF.

**Step 18.** The I-CSCF passes the 183 Session Progress message to the (ingress) IBCF.

**Step 19.** The (ingress) IBCF passes the SIP 183 Session Progress message to the originating network via the originating network IBCF.

**Step 20.** The LPG maps the SIP signaling from the incoming INVITE message to the outgoing Traditional or Enhanced MF signaling sequences and forwards the call to the legacy PSAP.

- For PSAPs that support a Traditional MF interface where delivery of callback information is preferred, the LPG will map the information received in the From/P-Asserted-Identity headers of the incoming SIP INVITE message, if that information is in the form of (or easily converted to) a 10-digit NANP number. If the callback information is not in the form of (or easily converted to) a 10-digit NANP number, the LPG will generate a pANI, following the procedures in Clause 6.2.2 of NENA-STA-010.3 [Ref 27]. The LPG will also allocate an appropriate NPD digit based on the NPA associated with the callback information/pANI. The

[18] If the PSAP expects delivery of a location key, or it expects the delivery of a callback number and the callback information received by the LPG in the SIP INVITE message is not in the form of, or easily converted to, a 10-digit NANP number, the LPG will generate a pANI.

LPG will then signal the NPD and 7-digit callback number or pANI in the MF ANI sequence KP + NPD + NXX XXXX + ST.

- For PSAPs that support a Traditional MF interface where delivery of location information is preferred, the LPG will generate a pANI and populate it, along with an appropriate NPD digit (i.e., the NPD + 7D pANI), in the MF ANI sequence KP + NPD + NXX XXXX + ST.
- For PSAPs that support an Enhanced MF interface with 10-digit delivery where delivery of callback information is preferred, the LPG will map the information received in the From/P-Asserted-Identity headers of the SIP INVITE message, if that information is in the form of (or easily converted to) a 10-digit NANP number. If the callback information is not in the form of (or easily converted to) a 10-digit NANP number, the LPG will generate a pANI, following the procedures in Clause 6.2.2 of NENA-STA-010.3 [Ref 27]. The LPG will allocate an appropriate II value and then signal the II digits plus the 10D pANI or 10D callback number to the PSAP in the MF ANI sequence KP + II + NPA NXX XXXX + ST´.
- For PSAPs that support an Enhanced MF interface with 10-digit delivery where delivery of location information is preferred, the LPG will generate a pANI and populate it, along with an appropriate II value (i.e., the II digits plus the 10D pANI), in the MF ANI sequence KP + II + NPA NXX XXXX + ST´.
- For PSAPs that support an Enhanced MF interface with 20-digit delivery, the LPG will map the pANI (representing the LbyV) that it generated and the callback information that it received in the From/PAI headers (or a pANI if the callback information is not in the form of, or easily converted to, a 10-digit NANP number), along with an II value allocated by the LPG, to the MF sequence KP + II + NPA NXX XXXX + ST + KP + NPA NXX XXXX + ST, where the first 10-digit number is associated with the callback information from the PAI/From headers and the second 10-digit number contains the pANI associated with the LbyV.[19]

**Step 21.** Audible ringing is returned by the legacy PSAP to the LPG.

**Step 22.** Audible ringing is passed to the originating network/caller.

**Step 23.** The legacy PSAP sends a location query to the LPG using a legacy ALI protocol. The ALI query includes the 10-digit pANI and/or callback number received in Step 20. (Note that this can happen any time after Step 20.)

**Step 24.** The LPG returns an ALI response to the legacy PSAP that includes location information, a callback number and other information (e.g., class of service), as appropriate for the interface.

**Step 25.** When the PSAP answers the call, it returns an off-hook signal to the LPG.

**Step 26.** In response to the off-hook signal, the LPG generates a SIP 200 OK message and passes it to the (egress) IBCF.

**Step 27.** The (egress) IBCF passes the SIP 200 OK message to the E-CSCF.

**Step 28.** (Conditional on Step 9) The E-CSCF sends a notification to the LRF updating the call state.

**Step 29.** The E-CSCF passes the SIP 200 OK message to the I-CSCF.

**Step 30.** The I-CSCF passes the SIP 200 OK message to the (ingress) IBCF.

**Step 31.** The (ingress) IBCF passes the SIP 200 OK message to the originating network via the originating network IBCF.

**Step 32.** At this point a two-way connection is established between the caller and the PSAP.

**Step 33.** At some point the call is terminated. In this call flow, the PSAP terminates the call and sends an on-hook indication to the LPG.

[19] Note that the same pANI value can be used to represent the location and the callback information.

**Step 34.** The LPG maps the on-hook indication to a SIP BYE message and sends the SIP BYE message to the (egress) IBCF.

**Step 35.** The (egress) IBCF passes the SIP BYE message to the E-CSCF.

**Step 36.** (Conditional on Step 9) The E-CSCF then notifies the LRF that the call has terminated.

**Step 37.** The E-CSCF passes the SIP BYE message to the (ingress) IBCF.

**Step 38.** The (ingress) IBCF passes the SIP BYE message to the originating network via the originating network IBCF.

## *8.4 IMS Originating Network to i3 and Legacy PSAPs – LbyR*

### 8.4.1 Delivery of Emergency Call Origination from IMS Origination Network to i3 PSAP with LbyR

The call flow provided in Figure 8-9 illustrates a scenario where an emergency call is delivered by an IMS origination network to an IMS-based NG9-1-1 Emergency Services Network with LbyR and Additional Data (by reference). The call is delivered to an IBCF on the ingress side of the IMS-based NG9-1-1 Emergency Services Network. The SIP INVITE message signaled by the IMS originating network includes a Route header that contains the URI of an I-CSCF in the IMS-based NG9-1-1 Emergency Services Network, an emergency services service URN (urn:service:sos) in the Request-URI, callback information in the P-Asserted-Identity header, a LbyR URI in the Geolocation header, and an Additional Data URI in the Call-info header. (A Geolocation-Routing header set to “yes”, and other SIP headers will also be included in the SIP INVITE message, but are not specifically illustrated in Figure 8-9.) In this example call flow, the I-CSCF forwards the SIP INVITE message to the E-CSCF which passes it to the LRF. The LRF de-references the received LbyR URI by sending a de-reference request to the LRF in the originating IMS network. The LRF then uses the LbyV received in the de-reference response to query the RDF. In this example flow, the Route URI that is returned by the RDF is assumed to be associated with an i3 PSAP. Figure 8-9 shows the emergency call then being delivered to the i3 PSAP with the same LbyR and Additional Data (by reference) as was received by the IMS-based NG9-1-1 Emergency Services Network in incoming signaling from the originating IMS network. (See Clause 8.12.1 for a call flow illustrating the application of SHAKEN caller identity authentication/verification and RPH signing/verification to an emergency call origination from an IMS origination network to an i3 PSAP.)

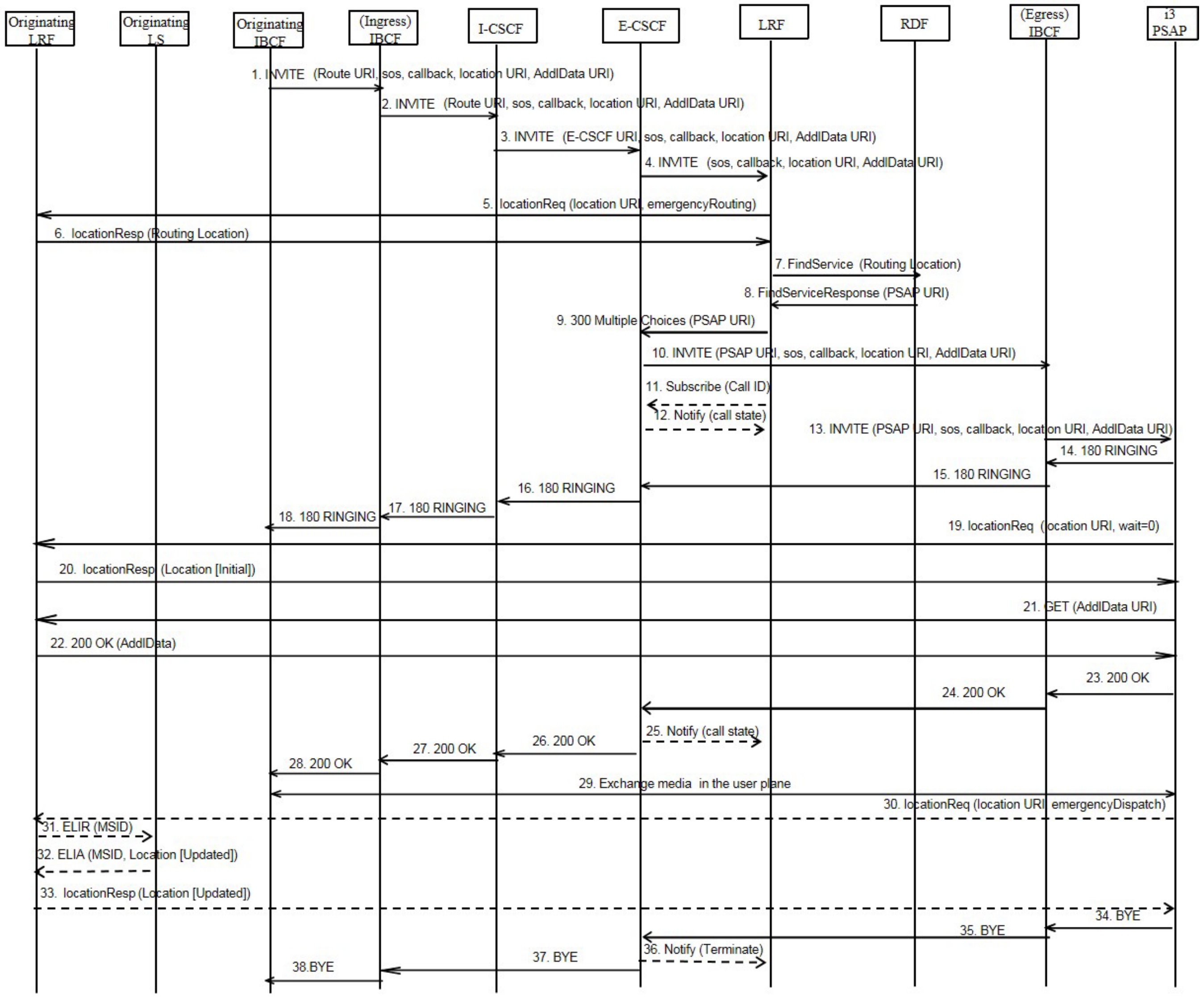

Originating LRF
Originating LS
Originating IBCF
(Ingress) IBCF
I-CSCF
E-CSCF
LRF
RDF
(Egress) IBCF
i3 PSAP
1. INVITE (Route URI, sos, callback, location URI, AddlData URI)
2. INVITE (Route URI, sos, callback, location URI, AddlData URI)
3. INVITE (E-CSCF URI, sos, callback, location URI, AddlData URI)
4. INVITE (sos, callback, location URI, AddlData URI)
5. locationReq (location URI, emergencyRouting)
6. locationResp (Routing Location)
7. FindService (Routing Location)
8. FindServiceResponse (PSAP URI)
9. 300 Multiple Choices (PSAP URI)
10. INVITE (PSAP URI, sos, callback, location URI, AddlData URI)
11. Subscribe (Call ID)
12. Notify (call state)
13. INVITE (PSAP URI, sos, callback, location URI, AddlData URI)
14. 180 RINGING
15. 180 RINGING
16. 180 RINGING
17. 180 RINGING
18. 180 RINGING
19. locationReq (location URI, wait=0)
20. locationResp (Location [Initial])
21. GET (AddlData URI)
22. 200 OK (AddlData)
23. 200 OK
24. 200 OK
25. Notify (call state)
26. 200 OK
27. 200 OK
28. 200 OK
29. Exchange media in the user plane
30. locationReq (location URI, emergencyDispatch)
31. ELIR (MSID)
32. ELIA (MSID, Location [Updated])
33. locationResp (Location [Updated])
34. BYE
35. BYE
36. Notify (Terminate)
37. BYE
38.BYE

**Figure 8.9: Delivery of IMS Emergency Call Origination to i3 PSAP with LbyR**

**Step 1.** The IBCF in the IMS originating network sends an emergency call origination to an (ingress) IBCF in the IMS-based NG9-1-1 Emergency Services Network. The SIP INVITE message includes a Route header that contains the I-CSCF URI, an emergency services service URN (urn:service:sos), callback information, a LbyR URI, and an Additional Data URI.

**Step 2.** The IBCF forwards the received INVITE message to the I-CSCF.

**Step 3.** The I-CSCF forwards the SIP INVITE to the pre-configured E-CSCF. The SIP INVITE message sent to the E-CSCF by the I-CSCF contains the E-CSCF URI in the Route header, and includes the callback information, “sos” service URN, LbyR URI, and Additional Data URI, as received in the incoming SIP INVITE message.

**Step 4.** The E-CSCF forwards the SIP INVITE to the LRF.

**Step 5.** In this example, the SIP INVITE contains a LbyR URI, so the LRF in the IMS-based NG9-1-1 Emergency Services Network queries the LRF in the IMS originating network (as identified in the LbyR URI) for the routing location (i.e., responseTime parameter = emergencyRouting).

**Step 6.** The originating LRF returns the Routing Location that is associated with the LbyR URI.

**Step 7.** The LRF queries the RDF using the location information obtained in Step 6 and the emergency service URN (urn:service:sos).

**Step 8.** The RDF returns a Route URI. In this example, the Route URI is associated with an i3 PSAP that is served by the IMS-based NG9-1-1 Emergency Services Network.

**Step 9.** The LRF redirects the call back to the E-CSCF, passing the Route (PSAP) URI.

**Step 10.** The E-CSCF generates an outgoing SIP INVITE message, using the information received from the LRF, as well as information received in the initial SIP INVITE message, and forwards it to the (egress) IBCF. The SIP INVITE message contains the PSAP URI in the Route header, the sos service URN in the Request-URI, the callback information in the From and P-Asserted-Identity headers, the LbyR URI in the Geolocation header, and an Additional Data URI in the Call-Info header. (A Geolocation-Routing header set to “yes” will also be present in the SIP INVITE message, as well as other SIP headers per RFC 3261 [Ref 18]).

**Step 11.** (Optional) The LRF may subscribe to the state of the call.

**Step 12.** (Conditional on Step 11) The E-CSCF sends an initial notification of the call state.

**Step 13.** The (egress) IBCF forwards the SIP INVITE message to the i3 PSAP with the callback information, LbyR URI, and Additional Data URI received by the IMS-based NG9-1-1 Emergency Services Network in the SIP INVITE message from the IMS originating network.

**Step 14.** An indication that the call taker is being alerted is returned by the i3 PSAP to the (egress) IBCF (using a SIP 180 RINGING message).

**Step 15.** The (egress) IBCF passes the SIP 180 RINGING message to the E-CSCF.

**Step 16.** The E-CSCF passes the SIP 180 RINGING message to the I-CSCF.

**Step 17.** The I-CSCF passes the SIP 180 RINGING message to the (ingress) IBCF.

**Step 18.** The (ingress) IBCF passes the SIP 180 RINGING message to the originating network via the originating network IBCF.

**Step 19.** Since the SIP INVITE message received by the i3 PSAP contains a LbyR, the i3 PSAP queries the LRF in the originating IMS network (as identified in the LbyR URI) for initial caller location (i.e., responseTime contains a wait timer value of “0”). (Note that this can occur any time after Step13.)

**Step 20.** The originating LRF supplies the initial caller location information to the PSAP. The initial display location information is displayed at the PSAP CPE.

**Step 21.** Since the SIP INVITE message received by the i3 PSAP contains Additional Data (by reference), the i3 PSAP queries the LRF in the originating IMS network using a GET request. (Note that this can occur any time after Step 13.)

**Step 22.** The originating LRF supplies the Additional Data (by value) to the PSAP.

**Step 23.** When the PSAP answers the call, it returns a SIP 200 OK message to the (egress) IBCF.

**Step 24.** The (egress) IBCF passes the SIP 200 OK message to the E-CSCF.

**Step 25.** (Conditional on Step 11) The E-CSCF sends a notification to the LRF updating the call state.

**Step 26.** The E-CSCF passes the SIP 200 OK message to the I-CSCF.

**Step 27.** The I-CSCF passes the SIP 200 OK message to the (ingress) IBCF.

**Step 28.** The (ingress) IBCF passes the SIP 200 OK message to the originating network via the originating network IBCF.

**Step 29.** At this point a two-way connection is established between the caller and the PSAP.

**Step 30.** (Optional) The PSAP queries the LRF in the originating IMS network (as identified in the LbyR URI) for updated (dispatch) location information (responseTime parameter = “emergencyDispatch” in this example).

**Step 31.** (Conditional on Step 30) The originating LRF queries the LS for updated (dispatch) location. (Note that the value of the responseTime parameter [emergencyDispatch or a specific time value] will be used by the LRF to determine whether to query the LS.)

**Step 32.** (Conditional on Step 31) The LS returns updated (dispatch) location information to the originating LRF.

**Step 33.** (Conditional on Step 30) The LRF in the IMS-based originating network supplies the updated (dispatch) location to the i3 PSAP and it is displayed on the PSAP CPE.

**Step 34.** At some point the call is terminated. In this call flow, the PSAP terminates the call and sends a SIP BYE message to the (egress) IBCF.

**Step 35.** The SIP BYE is passed from the (egress) IBCF to the E-CSCF.

**Step 36.** (Conditional on Step 11) The E-CSCF then notifies the LRF that the call has terminated.

**Step 37.** The E-CSCF passes the SIP BYE message to the (ingress) IBCF.

**Step 38.** The (ingress) IBCF passes the SIP BYE message to the originating network via the originating network IBCF.

### 8.4.2 Delivery of Emergency Call Origination from IMS Origination Network to Legacy PSAP with LbyR

The call flow provided in Figure 8-10 illustrates a scenario where an emergency call is delivered by an IMS origination network to an IMS-based NG9-1-1 Emergency Services Network with LbyR and Additional Data (by reference). The call is delivered to an IBCF on the ingress side of the IMS-based NG9-1-1 Emergency Services Network. The SIP INVITE message signaled by the IMS originating network includes a Route header that contains the URI of an I-CSCF in the IMS-based NG9-1-1 Emergency Services Network, an emergency services service URN (urn:service:sos) in the Request-URI, callback information in the P-Asserted-Identity header, a LbyR URI in the Geolocation header, and an Additional Data URI in the Call-info header. (A Geolocation-Routing header set to “yes”, and other SIP headers will also be included in the SIP INVITE message, per RFC 3261 [Ref 18]. These headers are not specifically illustrated in Figure 8-10.) This call flow assumes that the I-CSCF forwards the SIP INVITE message to the E-CSCF, and the E-CSCF forwards it to the LRF. The LRF de-references the received LbyR URI by sending a de-reference request to the LRF in the originating IMS network. The LRF then uses the LbyV received in the de-reference response to query the RDF. In this example call flow, the Route URI that is returned by the RDF is associated with a legacy PSAP. The call flow depicted in Figure 8-10 assumes that the LPG may generate a 7/10-digit pANI for the call and, based on per-PSAP provisioning, associates an appropriate Numbering Plan Digit (NPD) or ANI II value with the call (depending on whether the PSAP supports a Traditional MF interface or an Enhanced MF interface).

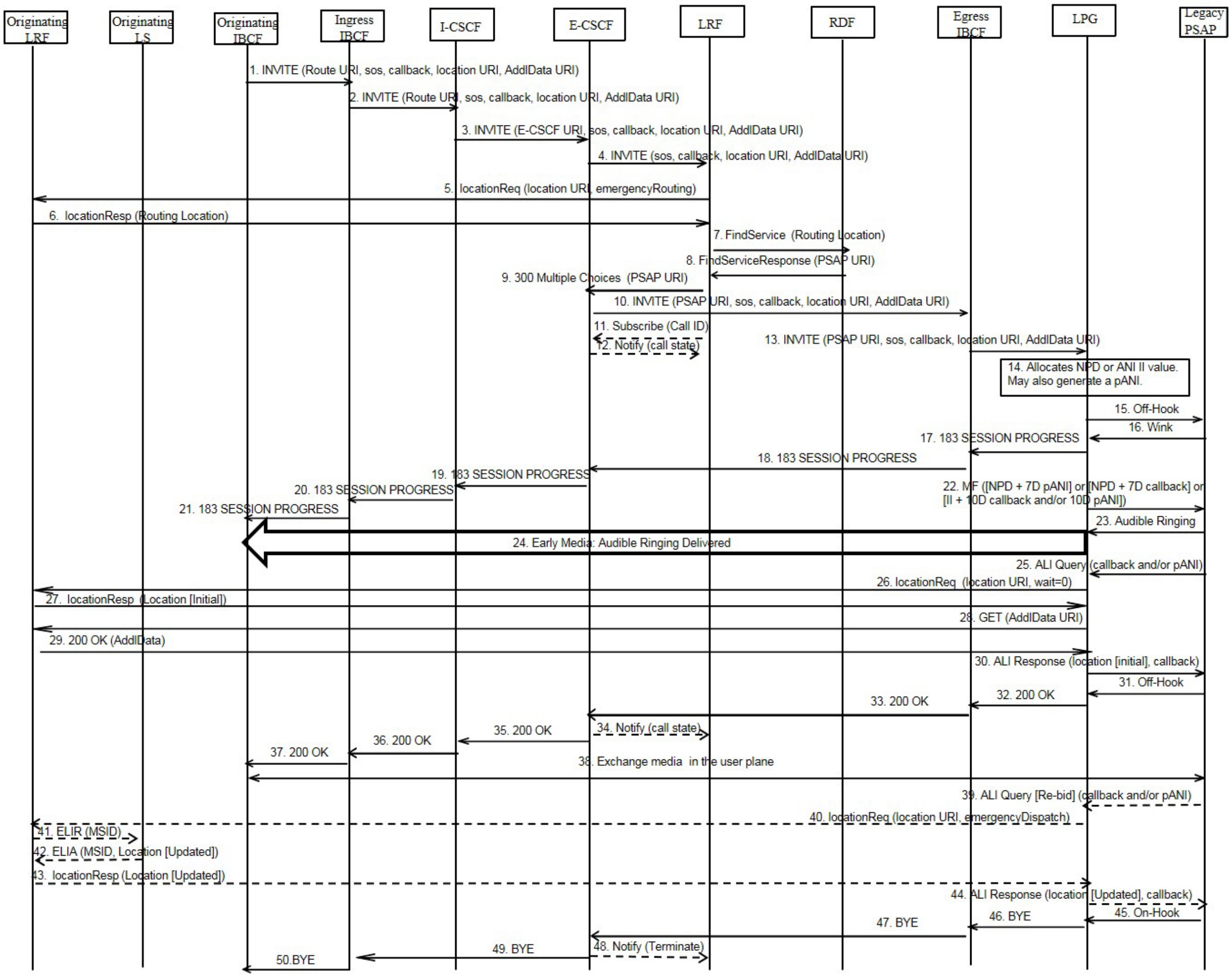

Originating LRF
Originating LS
Originating IBCF
Ingress IBCF
I-CSCF
E-CSCF
LRF
RDF
Egress IBCF
LPG
Legacy PSAP
1. INVITE (Route URI, sos, callback, location URI, AddlData URI)
2. INVITE (Route URI, sos, callback, location URI, AddlData URI)
3. INVITE (E-CSCF URI, sos, callback, location URI, AddlData URI)
4. INVITE (sos, callback, location URI, AddlData URI)
5. locationReq (location URI, emergencyRouting)
6. locationResp (Routing Location)
7. FindService (Routing Location)
8. FindServiceResponse (PSAP URI)
9. 300 Multiple Choices (PSAP URI)
10. INVITE (PSAP URI, sos, callback, location URI, AddlData URI)
11. Subscribe (Call ID)
12. Notify (call state)
13. INVITE (PSAP URI, sos, callback, location URI, AddlData URI)
14. Allocates NPD or ANI II value. May also generate a pANI.
15. Off-Hook
16. Wink
17. 183 SESSION PROGRESS
18. 183 SESSION PROGRESS
19. 183 SESSION PROGRESS
20. 183 SESSION PROGRESS
21. 183 SESSION PROGRESS
22. MF ([NPD + 7D pANI] or [NPD + 7D callback] or [II + 10D callback and/or 10D pANI])
23. Audible Ringing
24. Early Media: Audible Ringing Delivered
25. ALI Query (callback and/or pANI)
26. locationReq (location URI, wait=0)
27. locationResp (Location [Initial])
28. GET (AddlData URI)
29. 200 OK (AddlData)
30. ALI Response (location [initial], callback)
31. Off-Hook
32. 200 OK
33. 200 OK
34. Notify (call state)
35. 200 OK
36. 200 OK
37. 200 OK
38. Exchange media in the user plane
39. ALI Query [Re-bid] (callback and/or pANI)
40. locationReq (location URI, emergencyDispatch)
41. ELIR (MSID)
42. ELIA (MSID, Location [Updated])
43. locationResp (Location [Updated])
44. ALI Response (location [Updated], callback)
45. On-Hook
46. BYE
47. BYE
48. Notify (Terminate)
49. BYE
50.BYE

**Figure 8.10: Delivery of IMS Emergency Call Origination to Legacy PSAP with LbyR**

**Step 1.** The IBCF in the IMS originating network sends an emergency call origination to an (ingress) IBCF in the IMS-based NG9-1-1 Emergency Services Network. The SIP INVITE message includes a Route header that contains the I-CSCF URI, an emergency services service URN (urn:service:sos), callback information, a LbyR URI, and an Additional Data URI.

**Step 2.** The (ingress) IBCF forwards the received INVITE message to the I-CSCF.

**Step 3.** The I-CSCF forwards the SIP INVITE to the pre-configured E-CSCF. The SIP INVITE message sent to the E-CSCF by the I-CSCF contains the E-CSCF URI in the Route header, and includes the callback information, “sos” service URN, LbyR, and an Additional Data URI, as received in the incoming SIP INVITE message.

**Step 4.** The E-CSCF forwards the SIP INVITE to the LRF.

**Step 5.** In this example, the SIP INVITE contains a LbyR URI, so the LRF in the IMS-based NG9-1-1 Emergency Services Network queries the LRF in the IMS originating network (as identified in the location URI) for routing location (i.e., responseTime parameter = emergencyRouting).

**Step 6.** The originating LRF returns the Routing Location that is associated with the LbyR URI.

**Step 7.** The LRF queries the RDF using the location information obtained in Step 6 and the emergency service URN (urn:service:sos).

**Step 8.** The RDF returns a Route URI. In this example, the Route URI is associated with a legacy PSAP that is served by the IMS-based NG9-1-1 Emergency Services Network.

**Step 9.** The LRF redirects the call back to the E-CSCF, passing the Route (PSAP) URI.

**Step 10.** The E-CSCF generates an outgoing SIP INVITE message, using the information received from the LRF, as well as information received in the initial SIP INVITE message, and forwards it to the (egress) IBCF. The SIP INVITE message includes the PSAP URI in the Route header, the sos service URN in the Request-URI, the callback information in the From and P-Asserted-Identity headers, the LbyR URI in the Geolocation header, and an Additional Data URI in the Call-Info header. (A Geolocation-Routing header set to "yes" will also be present in the SIP INVITE message, as well as other SIP headers per RFC 3261 [Ref 18]).

**Step 11.** (Optional) The LRF may subscribe to the state of the call.

**Step 12.** (Conditional on Step 11) The E-CSCF sends an initial notification of the state.

**Step 13.** The (egress) IBCF forwards the SIP INVITE to the LPG.

**Step 14.** The LPG determines, based on provisioning, whether the PSAP associated with the received PSAP URI supports a Traditional MF or Enhanced MF interface. Depending on the type of interface supported by the PSAP, the LPG may generate a pANI and will assign an appropriate NPD or ANI II value to the call, following the procedures specified in Clause 6.2.2 of NENA-STA-010.3 [Ref 27].

**Step 15.** The LPG generates an off-hook signal toward the legacy PSAP.

**Step 16.** The legacy PSAP returns a wink signal back to the LPG.

**Step 17.** The LPG generates a 183 Session Progress message and sends it to the (egress) IBCF.

**Step 18.** The (egress) IBCF passes the 183 Session Progress message to the E-CSCF.

**Step 19.** The E-CSCF passes the 183 Session Progress message to the I-CSCF.

**Step 20.** The I-CSCF passes the 183 Session Progress message to the (ingress) IBCF.

**Step 21.** The (ingress) IBCF passes the SIP 183 Session Progress message to the originating network via the originating network IBCF.

**Step 22.** The LPG delivers the call to the legacy PSAP, mapping the SIP signaling from the incoming INVITE message to the outgoing Traditional or Enhanced MF signaling sequences.

- If the PSAP supports a Traditional MF interface and is provisioned to receive callback information, and the callback information received in the From/P-Asserted-Identity header is in the form of (or easily converted to) a NANP number with an NPA that is appropriate for the PSAP, the LPG will map the information received in the From/P-Asserted-Identity header of the incoming SIP INVITE message, and the NPD digit it derived in Step 14 (i.e., NPD + 7-digit callback information) to the MF ANI sequence KP + NPD + NXX XXXX + ST.
- If the PSAP supports a Traditional MF interface and is provisioned to receive callback information, and the callback information received by the LPG is not in the form of (or easily converted to) a NANP number with an NPA that is appropriate for the PSAP, the LPG will populate the pANI that it generated and the NPD digit that it derived in Step 14 (i.e., NPD + 7-digit pANI) in the MF ANI sequence KP + NPD + NXX XXXX + ST.
- If the PSAP supports a Traditional MF interface and is provisioned to receive location information, the LPG will populate the pANI that it generated and the NPD digit that it derived in Step 14 (i.e., NPD + 7-digit pANI) in the MF ANI sequence KP + NPD + NXX XXXX + ST.
- If the PSAP supports an Enhanced MF interface with 10-digit delivery, and is provisioned to receive callback information, and the callback information received by the LPG is in the form of (or easily converted to) a NANP number with an NPA that is appropriate for the PSAP, the LPG will map the information received in the From/P-Asserted-Identity header of

the SIP INVITE message, and the II digits it derived in Step 14 (i.e., II + 10-digit callback information) to the MF ANI sequence KP + II + NPA NXX XXXX + ST´.

- If the PSAP supports an Enhanced MF interface with 10-digit delivery, and is provisioned to receive callback information, and the callback information received by the LRF is not in the form of (or easily converted to) a NANP number with an NPA that is appropriate for the PSAP, the LPG will populate the pANI that it generated and the II digits that it derived in Step 14 (i.e., II + 10-digit pANI) in the MF ANI sequence KP + II + NPA NXX XXXX + ST´.
- If the PSAP supports an Enhanced MF interface with 10-digit delivery, and is provisioned to receive location information, the LPG will populate the pANI that it generated and the II digits that it derived in Step 14 (i.e., II + 10-digit pANI) in the MF ANI sequence KP + II + NPA NXX XXXX + ST´.
- For PSAPs that support an Enhanced MF interface with 20-digit delivery, where the callback information received by the LPG is in the form of (or easily converted to) a NANP number with an NPA that is appropriate for the PSAP, the LPG will map the information received in the From/P-Asserted-Identity header along with the II digits that it derived in Step 14 (i.e., II + 10-digit callback information), as well as the pANI that it generated in Step 14 to the MF sequence KP + II + NPA NXX XXXX + ST + KP + NPA NXX XXXX + ST, where the first 10-digit number is mapped from the From/P-Asserted-Identity header and the second 10-digit number contains the pANI generated in Step 14.
- For PSAPs that support an Enhanced MF interface with 20-digit delivery, where the callback information received by the LPG is not in the form of (or easily converted to) a NANP number with an NPA that is appropriate for the PSAP, the LPG will populate the pANI and the II digits that it derived in Step 14 (i.e., II + 10-digit pANI), as well as the pANI that it generated in Step 14 associated with the location information, to the MF sequence KP + II + NPA NXX XXXX + ST + KP + NPA NXX XXXX + ST, where the first 10-digit number is the pANI associated with the callback information and the second 10-digit number is pANI associated with the location information.

  NOTE: The same pANI value can be used to represent both callback information and location information, as specified in NENA-STA-010.3 [Ref 27].

**Step 23.** Audible ringing is returned by the legacy PSAP to the LPG.

**Step 24.** Audible ringing is passed to the originating network/caller.

**Step 25.** The legacy PSAP sends a location query to the LPG using a legacy ALI protocol. The ALI query includes the 10-digit callback information and/or pANI received in Step 22. (Note that this can happen any time after Step 22.)

**Step 26.** The LPG sends a de-reference request to the originating LRF (as identified in the LbyR URI associated with the Reference Identifier/callback information) for initial caller location (i.e., responseTime contains a wait timer value of “0”).

**Step 27.** The originating LRF supplies the initial caller location information to the LPG in the de-reference response.

**Step 28.** In this example, the SIP INVITE received by the LPG contains an Additional Data URI, so the LPG queries the originating LRF (as identified in the URI) for Additional Data using an HTTPS GET operation.

**Step 29.** The originating LRF provides the requested Additional Data in a 200 OK response.[20]

**Step 30.** The LPG returns an ALI response to the legacy PSAP that includes the initial caller location information, a callback number and other information (e.g., class of service), as appropriate for the interface.

[20] Note that Steps 26 through 29 can happen any time after Step 22, and that Steps 26 and 27 can be performed either before or after Steps 28 and 29.

**Step 31.** When the PSAP answers the call, it returns an off-hook signal to the LPG.

**Step 32.** In response to the off-hook signal, the LPG generates a SIP 200 OK message and passes it to the (egress) IBCF.

**Step 33.** The (egress) IBCF passes the SIP 200 OK message to the E-CSCF.

**Step 34.** (Conditional on Step 11) The E-CSCF sends a notification to the LRF updating the call state.

**Step 35.** The E-CSCF passes the SIP 200 OK message to the I-CSCF.

**Step 36.** The I-CSCF passes the SIP 200 OK message to the (ingress) IBCF.

**Step 37.** The (ingress) IBCF passes the SIP 200 OK message to the originating network via the originating network IBCF.

**Step 38.** At this point a two-way connection is established between the caller and the PSAP.

**Step 39.** (Optional) The legacy PSAP sends an ALI re-bid query (containing the callback information and/or pANI received in Step 22) to the LPG.

**Step 40.** (Optional) The LPG queries the originating LRF (as identified in the LbyR URI that is associated with the Reference Identifier) for updated (dispatch) location information (responseTime parameter = “emergencyDispatch” in this example).

**Step 41.** (Conditional on Step 40) The originating LRF queries the LS for updated (dispatch) location. (Note that the value of the responseTime parameter [emergencyDispatch or a specific time value] will be used by the LRF to determine whether to query the LS.)

**Step 42.** (Conditional on Step 41) The LS returns updated (dispatch) location information to the originating LRF.

**Step 43.** (Conditional on Step 40) The LRF in the IMS-based originating network supplies updated (dispatch) location to the LPG.

**Step 44.** (Conditional on Step 39) The LPG supplies updated (dispatch) location (along with callback and other non-location information, as appropriate for the interface) for display at the legacy PSAP.

**Step 45.** At some point the call is terminated. In this call flow, the PSAP terminates the call and sends an on-hook indication to the LPG.

**Step 46.** The LPG maps the on-hook indication to a SIP BYE message and sends the SIP BYE message to the (egress) IBCF.

**Step 47.** The (egress) IBCF passes the SIP BYE message to the E-CSCF.

**Step 48.** (Conditional on Step 11) The E-CSCF then notifies the LRF that the call has terminated.

**Step 49.** The E-CSCF passes the SIP BYE message to the (ingress) IBCF.

**Step 50.** The (ingress) IBCF passes the SIP BYE message to the originating network via the originating network IBCF.

## *8.5 Non-IMS Originating Network to i3 and Legacy PSAPs – LbyV*

### 8.5.1 Delivery of Emergency Call Origination from Non-IMS VoIP Origination Network to i3 PSAP with LbyV

The call flow provided in Figure 8-11 illustrates a scenario where an emergency call is delivered by a non-IMS VoIP origination network to an IMS-based NG9-1-1 Emergency Services Network with LbyV. Upon detecting an emergency origination, the calling device requests location by querying a Location Information Server (LIS)[21] in the access network, using the HELD protocol. The HELD locationRequest contains an identifier associated with the calling device and appropriate credentials. It also contains an indication of the form that the provided location information should take. In this example call flow, the device requests a civic or geodetic location. The LIS responds with location information (i.e., LbyV). The device uses the location information returned in the HELD locationResponse to query an Emergency Call Routing Function (ECRF) for routing information. The ECRF returns a URI associated with the I-CSCF in an IMS-based NG9-1-1 Emergency Services Network. The device forwards the emergency session request to a Call Server/Proxy in its serving non-IMS i3-compliant originating network. The SIP INVITE message signaled by the device to the Call Server/Proxy includes a Route header that contains the URI of an I-CSCF in the IMS-based NG9-1-1 Emergency Services Network, an emergency services service URN (urn:service:sos) in the Request-URI, callback information in the P-Asserted-Identity header, and LbyV in the message body. (A Geolocation header that contains a Content-ID (cid) pointing to the PIDF-LO in the message body, a Geolocation-Routing header set to “yes”, and other SIP headers will also be included in the SIP INVITE message, but are not specifically illustrated in Figure 8-11.) The Call Server/Proxy adds Additional Data “by value” to the body of the SIP INVITE message, along with a Call-Info header that contains a cid pointing to the Additional Data in the message body, and forwards the SIP INVITE to an IBCF on the ingress side of the IMS-based NG9-1-1 Emergency Services Network. The IBCF forwards the SIP INVITE to the I-CSCF, and the I-CSCF forwards the SIP INVITE message to the pre-configured E-CSCF, populating the E-CSCF URI in the Route header. The E-CSCF forwards the SIP INVITE to the LRF. The LRF uses the LbyV to query the RDF. In this example call flow, the Route URI that is returned by the RDF is associated with an i3 PSAP. Figure 8-11 shows the emergency call then being delivered to the i3 PSAP with the same LbyV as was received by the IMS-based NG9-1-1 Emergency Services Network in incoming signaling from the non-IMS originating network, as well as Additional Data (by value). (See Clause 8.12.2 for a call flow illustrating the application of SHAKEN caller identity authentication/verification and RPH/SIP Priority header signing/verification to an emergency call origination from a non-IMS origination network to an i3 PSAP.)

[21] NENA defines a LIS as a functional element that provides the locations of endpoints either by-reference or by-value, and if by-value, in geo or civic format. A LIS can be queried by an endpoint for its own location or by another entity for the location of an endpoint. The LIS is also the entity that provides the dereferencing service, exchanging a location reference for a location value.

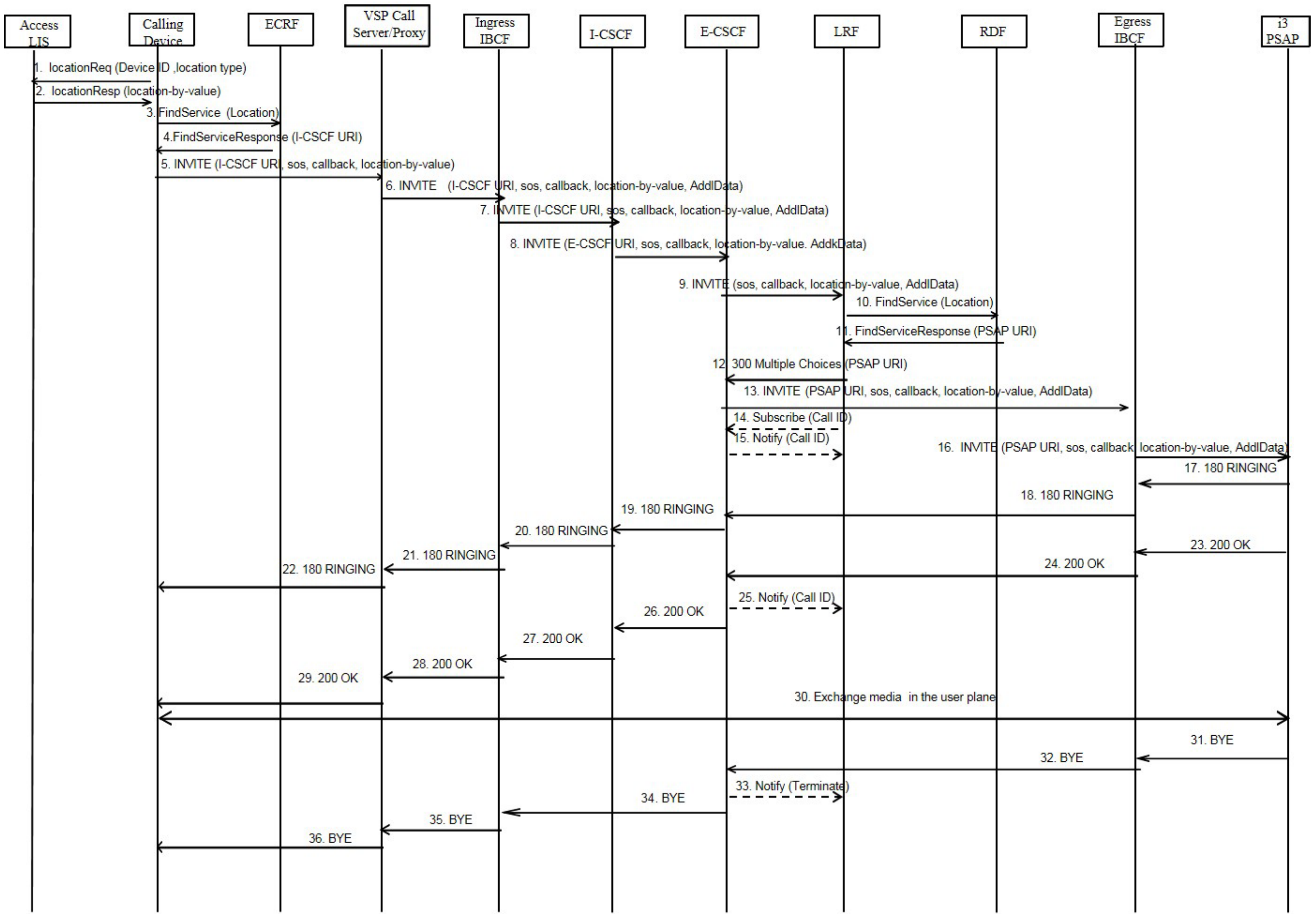

Access LIS
Calling Device
ECRF
VSP Call Server/Proxy
Ingress IBCF
I-CSCF
E-CSCF
LRF
RDF
Egress IBCF
i3 PSAP
1. locationReq (Device ID ,location type)
2. locationResp (location-by-value)
3. FindService (Location)
4.FindServiceResponse (I-CSCF URI)
5. INVITE (I-CSCF URI, sos, callback, location-by-value)
6. INVITE (I-CSCF URI, sos, callback, location-by-value, AddlData)
7. INVITE (I-CSCF URI, sos, callback, location-by-value, AddlData)
8. INVITE (E-CSCF URI, sos, callback, location-by-value. AddkData)
9. INVITE (sos, callback, location-by-value, AddlData)
10. FindService (Location)
11. FindServiceResponse (PSAP URI)
12. 300 Multiple Choices (PSAP URI)
13. INVITE (PSAP URI, sos, callback, location-by-value, AddlData)
14. Subscribe (Call ID)
15. Notify (Call ID)
16. INVITE (PSAP URI, sos, callback, location-by-value, AddlData)
17. 180 RINGING
18. 180 RINGING
19. 180 RINGING
20. 180 RINGING
21. 180 RINGING
22. 180 RINGING
23. 200 OK
24. 200 OK
25. Notify (Call ID)
26. 200 OK
27. 200 OK
28. 200 OK
29. 200 OK
30. Exchange media in the user plane
31. BYE
32. BYE
33. Notify (Terminate)
34. BYE
35. BYE
36. BYE

**Figure 8.11: Delivery of Non-IMS Emergency Call Origination to i3 PSAP with LbyV**

**Step 1.** Upon recognizing a request for emergency service, the calling device requests location by querying the LIS in the access network. (This example illustrates the use of the HELD protocol for the location request.) The locationRequest contains an identifier and appropriate credentials associated with the calling device, as well as an indication of the type of location being requested. In this example, the device requests civic or geodetic location. The locationRequest also includes a responseTime parameter (not shown) indicating how long the device is prepared to wait for a response or the purpose for which the device needs the location.

**Step 2.** The LIS responds to the location request by returning location information “by-value”.

**Step 3.** The device uses the LbyV in the location response from the LIS and the emergency service URN (urn:service:sos) to query an ECRF for routing information.

**Step 4.** The ECRF responds by returning a URI associated with an I-CSCF in an IMS-based NG9-1-1 Emergency Services Network.

**Step 5.** The device generates a SIP INVITE message that includes a Route header that contains the I-CSCF URI, an emergency services service URN (urn:service:sos), callback information, and LbyV (i.e., a Geolocation header that contains a cid, a Geolocation-Routing header set to “yes”, and a PIDF-LO in the body of the message that contains the LbyV), and sends it to a Call Server/Proxy in its serving non-IMS originating network.

**Step 6.** The Call Server/Proxy adds Additional Data “by value” to the received SIP INVITE message by including a Call-Info header that contains a cid pointing to the Additional Data in the message body, and forwards the SIP INVITE message to an IBCF on the ingress side of the IMS-based NG9-1-1 Emergency Services Network.

**Step 7.** The (ingress) IBCF forwards the received INVITE message to the I-CSCF.

**Step 8.** The I-CSCF determines the address of the E-CSCF (based on provisioned data) and forwards the SIP INVITE message to it. The SIP INVITE message sent to the E-CSCF by the I-CSCF contains the E-CSCF URI in the Route header, and includes the callback information, "sos" service URN, LbyV, and Additional Data "by value" as received in the incoming SIP INVITE message.

**Step 9.** The E-CSCF forwards the SIP INVITE to the LRF.

**Step 10.** The LRF queries the RDF using the location information received in the body of the received SIP INVITE message and the emergency service URN (urn:service:sos).

**Step 11.** The RDF returns a Route URI. In this example, the Route URI is associated with an i3 PSAP that is served by the IMS-based NG9-1-1 Emergency Services Network.

**Step 12.** The LRF redirects the call back to the E-CSCF, passing the Route (PSAP) URI.

**Step 13.** The E-CSCF generates an outgoing SIP INVITE message, using the information received from the LRF as well as information received in the initial SIP INVITE message, and forwards it to the (egress) IBCF. The SIP INVITE message contains the PSAP URI in the Route header, the sos service URN in the Request-URI, the callback information in the From and P-Asserted-Identity headers, the LbyV in the body (along with a cid in the Geolocation header and a Geolocation-Routing header set to "yes"), and Additional Data (by value) in the body (along with a cid in the Call-Info header).

**Step 14.** (Optional) The LRF may subscribe to the state of the call.

**Step 15.** (Conditional on Step 14) The E-CSCF sends an initial notification of the call state.

**Step 16.** The (egress) IBCF forwards the SIP INVITE message to the i3 PSAP with the callback information, the LbyV, and Additional Data received in the initial SIP INVITE message from the IMS originating network.

**Step 17.** An indication that the call taker is being alerted is returned by the i3 PSAP to the (egress) IBCF (using a SIP 180 RINGING message).

**Step 18.** The IBCF passes the SIP 180 RINGING message to the E-CSCF.

**Step 19.** The E-CSCF passes the SIP 180 RINGING message to the I-CSCF.

**Step 20.** The I-CSCF passes the SIP 180 RINGING message to the (ingress) IBCF.

**Step 21.** The (ingress) IBCF passes the SIP 180 RINGING message to the Call Server/Proxy in the non-IMS originating network.

**Step 22.** The Call Server/Proxy passes the SIP 180 RINGING message to the calling device.

**Step 23.** When the PSAP answers the call, it returns a SIP 200 OK message to the (egress) IBCF.

**Step 24.** The (egress) IBCF passes the SIP 200 OK message to the E-CSCF.

**Step 25.** (Conditional on Step 14) The E-CSCF sends a notification to the LRF updating the call state.

**Step 26.** The E-CSCF passes the SIP 200 OK message to the I-CSCF.

**Step 27.** The I-CSCF passes the SIP 200 OK message to the (ingress) IBCF.

**Step 28.** The (ingress) IBCF passes the SIP 200 OK message to the Call Server/Proxy in the non-IMS originating network.

**Step 29.** The Call Server/Proxy passes the SIP 200 OK message to the calling device.

**Step 30.** At this point a two-way connection is established between the caller and the PSAP.

**Step 31.** At some point the call is terminated. In this call flow, the PSAP terminates the call and sends a SIP BYE message to the (egress) IBCF.

**Step 32.** The SIP BYE is passed from the (egress) IBCF to the E-CSCF.

**Step 33.** (Conditional on Step 14) The E-CSCF then notifies the LRF that the call has terminated.

**Step 34.** The E-CSCF passes the SIP BYE message to the (ingress) IBCF.

**Step 35.** The (ingress) IBCF passes the SIP BYE message to the Call Server/Proxy in the non-IMS originating network.

**Step 36.** The Call Server/Proxy passes the SIP BYE message to the calling device.

### 8.5.2 Delivery of Emergency Call Origination from Non-IMS VoIP Origination Network to Legacy PSAP with LbyV

The call flow provided in Figure 8-12 illustrates a scenario where an emergency call is delivered by a non-IMS VoIP origination network to an IMS-based NG9-1-1 Emergency Services Network with LbyV. Upon detecting an emergency origination, the calling device requests location by querying a Location Information Server (LIS) in the access network, using the HELD protocol. The HELD locationRequest contains an identifier associated with the calling device and appropriate credentials. It also contains an indication of the form that the provided location information should take. In this example call flow, the device requests a civic or geodetic location. The LIS responds with location information (i.e., LbyV). The device uses the location information returned in the HELD locationResponse to query an Emergency Call Routing Function (ECRF) for routing information. The ECRF returns a URI associated with the I-CSCF in an IMS-based NG9-1-1 Emergency Services Network. The device forwards the emergency session request to a Call Server/Proxy in its serving non-IMS i3-compliant originating network. The SIP INVITE message signaled by the device to the Call Server/Proxy includes a Route header that contains the URI of an I-CSCF in the IMS-based NG9-1-1 Emergency Services Network, an emergency services service URN (urn:service:sos) in the Request-URI, callback information in the P-Asserted-Identity header, and LbyV in the message body. (A Geolocation header that contains a Content-ID (cid) pointing to the PIDF-LO in the message body, a Geolocation-Routing header set to “yes”, and other SIP headers will also be included in the SIP INVITE message, but are not specifically illustrated in Figure 8-12.) The Call Server/Proxy adds Additional Data “by value” to the body of the SIP INVITE message, along with a Call-Info header that contains a cid pointing to the Additional Data in the message body, and forwards the SIP INVITE to an IBCF on the ingress side of the IMS-based NG9-1-1 Emergency Services Network. The (ingress) IBCF forwards the SIP INVITE to the I-CSCF, and the I-CSCF forwards the SIP INVITE message to the pre-configured E-CSCF, populating the E-CSCF URI in the Route header. The E-CSCF forwards the SIP INVITE to the LRF. The LRF uses the LbyV to query the RDF. In this example call flow, the Route URI that is returned by the RDF is associated with a legacy PSAP. The call is forwarded via an (egress) IBCF to an i3 LPG with the LbyV and Additional Data (by value) that was provided to the IMS-based NG9-1-1 Emergency Services Network by the non-IMS originating network. In the call flow depicted in Figure 8-12, the LPG may generate a 7/10-digit pANI for the call and, based on per-PSAP provisioning, associates an appropriate Numbering Plan Digit (NPD) or ANI II value with the call (depending on whether the PSAP supports a Traditional MF interface or an Enhanced MF interface).

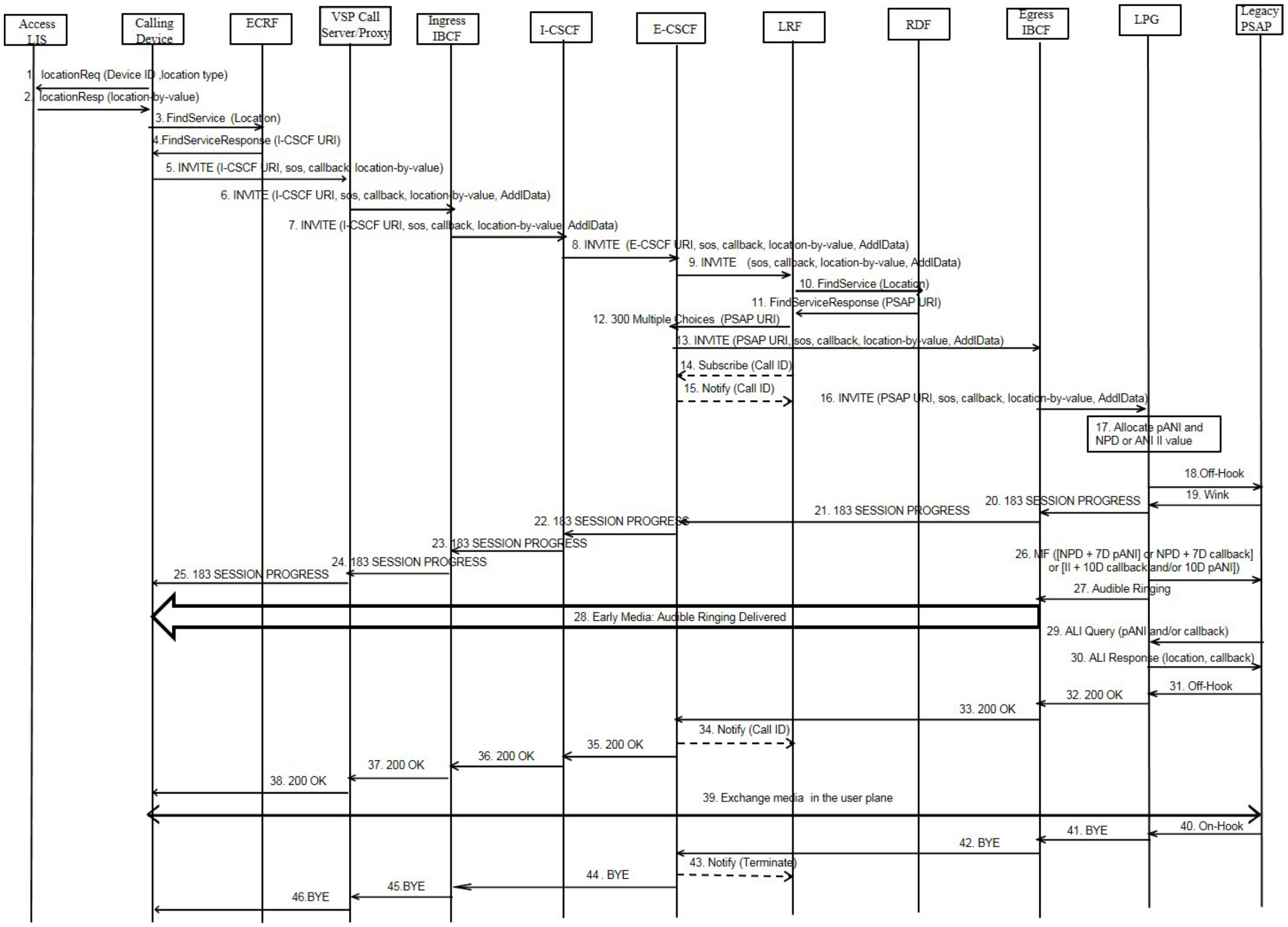

Access LIS
Calling Device
ECRF
VSP Call Server/Proxy
Ingress IBCF
I-CSCF
E-CSCF
LRF
RDF
Egress IBCF
LPG
Legacy PSAP
1. locationReq (Device ID ,location type)
2. locationResp (location-by-value)
3. FindService (Location)
4.FindServiceResponse (I-CSCF URI)
5. INVITE (I-CSCF URI, sos, callback, location-by-value)
6. INVITE (I-CSCF URI, sos, callback, location-by-value, AddlData)
7. INVITE (I-CSCF URI, sos, callback, location-by-value, AddlData)
8. INVITE (E-CSCF URI, sos, callback, location-by-value, AddlData)
9. INVITE (sos, callback, location-by-value, AddlData)
10. FindService (Location)
11. FindServiceResponse (PSAP URI)
12. 300 Multiple Choices (PSAP URI)
13. INVITE (PSAP URI, sos, callback, location-by-value, AddlData)
14. Subscribe (Call ID)
15. Notify (Call ID)
16. INVITE (PSAP URI, sos, callback, location-by-value, AddlData)
17. Allocate pANI and NPD or ANI II value
18.Off-Hook
19. Wink
20. 183 SESSION PROGRESS
21. 183 SESSION PROGRESS
22. 183 SESSION PROGRESS
23. 183 SESSION PROGRESS
24. 183 SESSION PROGRESS
25. 183 SESSION PROGRESS
26. MF ([NPD + 7D pANI] or NPD + 7D callback] or [II + 10D callback and/or 10D pANI])
27. Audible Ringing
28. Early Media: Audible Ringing Delivered
29. ALI Query (pANI and/or callback)
30. ALI Response (location, callback)
31. Off-Hook
32. 200 OK
33. 200 OK
34. Notify (Call ID)
35. 200 OK
36. 200 OK
37. 200 OK
38. 200 OK
39. Exchange media in the user plane
40. On-Hook
41. BYE
42. BYE
43. Notify (Terminate)
44 . BYE
45.BYE
46.BYE

**Figure 8.12: Delivery of Non-IMS Emergency Call Origination to Legacy PSAP with LbyV**

**Step 1.** Upon recognizing a request for emergency service, the calling device requests location by querying the LIS in the access network. (This example illustrates the use of the HELD protocol for the location request.) The locationRequest contains an identifier and appropriate credentials associated with the calling device, as well as an indication of the type of location being requested. In this example, the device requests civic or geodetic location. The locationRequest also includes a responseTime parameter (not shown) indicating how long the device is prepared to wait for a response or the purpose for which the device needs the location.

**Step 2.** The LIS responds to the location request by returning location information "by-value".

**Step 3.** The device uses the LbyV in the location response from the LIS and the emergency service URN (urn:service:sos) to query an ECRF for routing information.

**Step 4.** The ECRF responds by returning a URI associated with an I-CSCF in an IMS-based NG9-1-1 Emergency Services Network.

**Step 5.** The device generates a SIP INVITE message that includes a Route header that contains the I-CSCF URI, an emergency services service URN (urn:service:sos), callback information, and LbyV (i.e., a Geolocation header that contains a cid, a Geolocation-Routing header set to "yes" and a PIDF-LO in the body of the message that contains the LbyV), and sends it to a Call Server/Proxy in its serving non-IMS originating network.

**Step 6.** The Call Server/Proxy adds Additional Data (by value) to the received SIP INVITE message by including a Call-Info header that contains a cid pointing to the Additional Data in the message body, and forwards the SIP INVITE message to an IBCF on the ingress side of the IMS-based NG9-1-1 Emergency Services Network.

**Step 7.** The IBCF forwards the received INVITE message to the I-CSCF.

**Step 8.** The I-CSCF determines the address of the E-CSCF (based on provisioned data) and forwards the SIP INVITE message to it. The SIP INVITE message sent to the E-CSCF by the I-CSCF contains the E-CSCF URI in the Route header, and includes the callback information, “sos” service URN, LbyV, and Additional Data (by value) as received in the incoming SIP INVITE message.

**Step 9.** The E-CSCF forwards the SIP INVITE to the LRF.

**Step 10.** The LRF queries the RDF using the location information received in the body of the received SIP INVITE message and the emergency service URN (urn:service:sos).

**Step 11.** The RDF returns a Route URI. In this example, the Route URI is associated with a legacy PSAP that is served by the IMS-based NG9-1-1 Emergency Services Network.

**Step 12.** The LRF redirects the call back to the E-CSCF, passing the Route (PSAP) URI.

**Step 13.** The E-CSCF generates an outgoing SIP INVITE message, using the information received from the LRF, as well as information received in the initial SIP INVITE message, and forwards it to the (egress) IBCF. The SIP INVITE message includes the PSAP URI in the Route header, the sos service URN in the Request-URI, the callback information in the From and P-Asserted-Identity headers, the LbyV in the body (along with a cid in the Geolocation header and a Geolocation-Routing header set to “yes”), and Additional Data (by value) in the body (along with a cid in the Call-Info header).

**Step 14.** (Optional) The LRF may subscribe to the state of the call.

**Step 15.** (Conditional on Step 14) The E-CSCF sends an initial notification of the call state.

**Step 16.** The (egress) IBCF forwards the SIP INVITE message to the LPG.

**Step 17.** The LPG determines, based on provisioning, whether the PSAP associated with the received PSAP URI supports a Traditional MF or Enhanced MF interface. Depending on the type of interface supported by the PSAP, the LPG may generate a pANI[22] and will assign an appropriate NPD or ANI II value to the call, following the procedures specified in Clause 6.2.2 of NENA-STA-010.3 [Ref 27].

**Step 18.** The LPG generates an off-hook signal toward the legacy PSAP.

**Step 19.** The legacy PSAP returns a wink signal back to the LPG.

**Step 20.** The LPG generates a 183 Session Progress message and sends it to the (egress) IBCF.

**Step 21.** The (egress) IBCF passes the 183 Session Progress message to the E-CSCF.

**Step 22.** The E-CSCF passes the 183 Session Progress message to the I-CSCF.

**Step 23.** The I-CSCF passes the 183 Session Progress message to the (ingress) IBCF.

**Step 24.** The (ingress) IBCF passes the SIP 183 Session Progress message to Call Server/Proxy in the non-IMS originating network.

**Step 25.** The Call Server/Proxy passes the SIP 183 Session Progress message to the calling device.

**Step 26.** The LPG delivers the call to the legacy PSAP, mapping the SIP signaling from the incoming INVITE message to the outgoing Traditional or Enhanced MF signaling sequences.

[22] If the PSAP expects delivery of a location key, or it expects the delivery of a callback number and the callback information received by the LPG in the SIP INVITE message is not in the form of, or easily converted to, a 10-digit NANP number, the LPG will generate a pANI.

- For PSAPs that support a Traditional MF interface where delivery of callback information is preferred, the LPG will map the information received in the From/P-Asserted-Identity headers of the incoming SIP INVITE message, if that information is in the form of (or easily converted to) a 10-digit NANP number with an appropriate NPA value. If the callback information is not in the form of (or easily converted to) a 10-digit NANP number, the LPG will populate the pANI generated in Step 17 in the outgoing MF signaling sequence. The outgoing signaling will also include the NPD value obtained in Step 17. The LPG will signal the NPD and 7-digit callback number or pANI in the MF ANI sequence KP + NPD + NXX XXXX + ST.
- For PSAPs that support a Traditional MF interface where delivery of location information is preferred, the LPG will populate the pANI generated in Step 17, along with an appropriate NPD digit (i.e., NPD + 7D pANI) in the MF ANI sequence KP + NPD + NXX XXXX + ST.
- For PSAPs that support an Enhanced MF interface with 10-digit delivery where delivery of callback information is preferred, the LPG will map the information received in the From/P-Asserted-Identity headers of the SIP INVITE message, if that information is in the form of (or easily converted to) a 10-digit NANP number with an appropriate NPA. If the callback information is not in the form of (or easily converted to) a 10-digit NANP number, the LPG will signal the pANI, generated in Step 17 in the outgoing MF signaling sequence. The LPG will signal the II digits derived in Step 17 plus the 10D pANI or 10D callback number to the PSAP in the MF ANI sequence KP + II + NPA NXX XXXX + ST´.
- For PSAPs that support an Enhanced MF interface with 10-digit delivery where delivery of location information is preferred, the LPG will populate the pANI it generated in Step 17, along with an appropriate II value (i.e., II digits plus the 10D pANI), in the MF ANI sequence KP + II + NPA NXX XXXX + ST´.
- For PSAPs that support an Enhanced MF interface with 20-digit delivery, the LPG will populate the pANI (representing the LbyV) that it generated in Step 17 and the callback information that it received in the From/PAI headers (or a pANI if the callback information is not in the form of, or easily converted to, a 10-digit NANP number), along with the II value allocated by the LPG in Step 17, to the MF sequence KP + II + NPA NXX XXXX + ST + KP + NPA NXX XXXX + ST, where the first 10-digit number is associated with the callback information from the PAI/From headers and the second 10-digit number contains the pANI associated with the LbyV.

**Step 27.** Audible ringing is returned by the legacy PSAP to the LPG.

**Step 28.** Audible ringing is passed to the originating device/caller.

**Step 29.** The legacy PSAP sends a location query to the LPG using a legacy ALI protocol. The ALI query includes the 10-digit callback information and/or pANI received in Step 26. (Note that this can happen any time after Step 26.)

**Step 30.** The LPG returns an ALI response to the legacy PSAP that includes location information, a callback number and other information (e.g., class of service), as appropriate for the interface.

**Step 31.** When the PSAP answers the call, it returns an off-hook signal to the LPG.

**Step 32.** In response to the off-hook signal, the LPG generates a SIP 200 OK message and passes it to the (egress) IBCF.

**Step 33.** The (egress) IBCF passes the SIP 200 OK message to the E-CSCF.

**Step 34.** (Conditional on Step 14) The E-CSCF sends a notification to the LRF updating the call state.

**Step 35.** The E-CSCF passes the SIP 200 OK message to the I-CSCF.

**Step 36.** The I-CSCF passes the SIP 200 OK message to the (ingress) IBCF.

**Step 37.** The (ingress) IBCF passes the SIP 200 OK message to the Call Server/Proxy in the non-IMS originating network.

**Step 38.** The Call Server/Proxy passes the SIP 200 OK message to the calling device.

**Step 39.** At this point a two-way connection is established between the caller and the PSAP.

**Step 40.** At some point the call is terminated. In this call flow, the PSAP terminates the call and sends an on-hook indication to the LPG.

**Step 41.** The LPG maps the on-hook indication to a SIP BYE message and sends the SIP BYE message to the (egress) IBCF.

**Step 42.** The (egress) IBCF passes the SIP BYE message to the E-CSCF.

**Step 43.** (Conditional on Step 14) The E-CSCF then notifies the LRF that the call has terminated.

**Step 44.** The E-CSCF passes the SIP BYE message to the (ingress) IBCF.

**Step 45.** The (ingress) IBCF passes the SIP BYE message to the Call Server/Proxy in the non-IMS originating network.

**Step 46.** The Call Server/Proxy passes the SIP BYE message to the calling device.

## *8.6 Non-IMS VoIP Originating Network to i3 and Legacy PSAPs – LbyR*

### 8.6.1 Delivery of Emergency Call Origination from Non-IMS Origination Network to i3 PSAP with LbyR

The call flow provided in Figure 8-13 illustrates a scenario where an emergency call is delivered by a non-IMS i3-compliant VoIP origination network to an IMS-based NG9-1-1 Emergency Services Network with LbyR. Upon detecting an emergency origination, the calling device requests location by querying a Location Information Server (LIS) in the access network, using the HELD protocol. The HELD locationRequest contains an identifier associated with the calling device and appropriate credentials. It also contains an indication of the form that the provided location information should take. In this example call flow, the device requests geodetic location and a location URI. The LIS responds with geodetic location information and a location URI. The device uses the geodetic location returned in the HELD locationResponse to query an Emergency Call Routing Function (ECRF) for routing information. The ECRF returns a URI associated with the I-CSCF in an IMS-based NG9-1-1 Emergency Services Network. The device forwards the emergency session request to a Call Server/Proxy in its serving non-IMS, i3-compliant originating network. The SIP INVITE message signaled by the device to the Call Server/Proxy includes a Route header that contains the URI of an I-CSCF in the IMS-based NG9-1-1 Emergency Services Network, an emergency services service URN (urn:service:sos) in the Request-URI, callback information in the P-Asserted-Identity header, and a LbyR URI in the Geolocation header. (A Geolocation-Routing header set to “yes”, and other SIP headers will also be included in the SIP INVITE message, but are not specifically illustrated in Figure 8-13.) The Call Server/Proxy adds Additional Data “by reference” to the SIP INVITE message by including a Call-Info header that contains an Additional Data URI, and forwards the SIP INVITE to an IBCF on the ingress side of the IMS-based NG9-1-1 Emergency Services Network. The IBCF forwards the SIP INVITE to the I-CSCF, and the I-CSCF forwards the SIP INVITE message to the pre-configured E-CSCF, populating the E-CSCF URI in the Route header. The E-CSCF forwards the SIP INVITE to the LRF. The LRF de-references the received location URI by sending a de-reference request to the LIS in the access network. The LRF then uses the LbyV received in the de-reference response to query the RDF. The Route URI that is returned by the RDF is assumed to be associated with an i3 PSAP. Figure 8-13 shows the emergency call then being delivered to the i3 PSAP with the same LbyR and Additional Data “by reference” as was received by the IMS-based NG9-1-1 Emergency Services Network in incoming signaling from the non-IMS originating network. (See Clause 8.12.2 for a call flow illustrating the application of SHAKEN caller identity authentication/verification and RPH signing/verification to an emergency call origination from a non-IMS origination network to an i3 PSAP.)

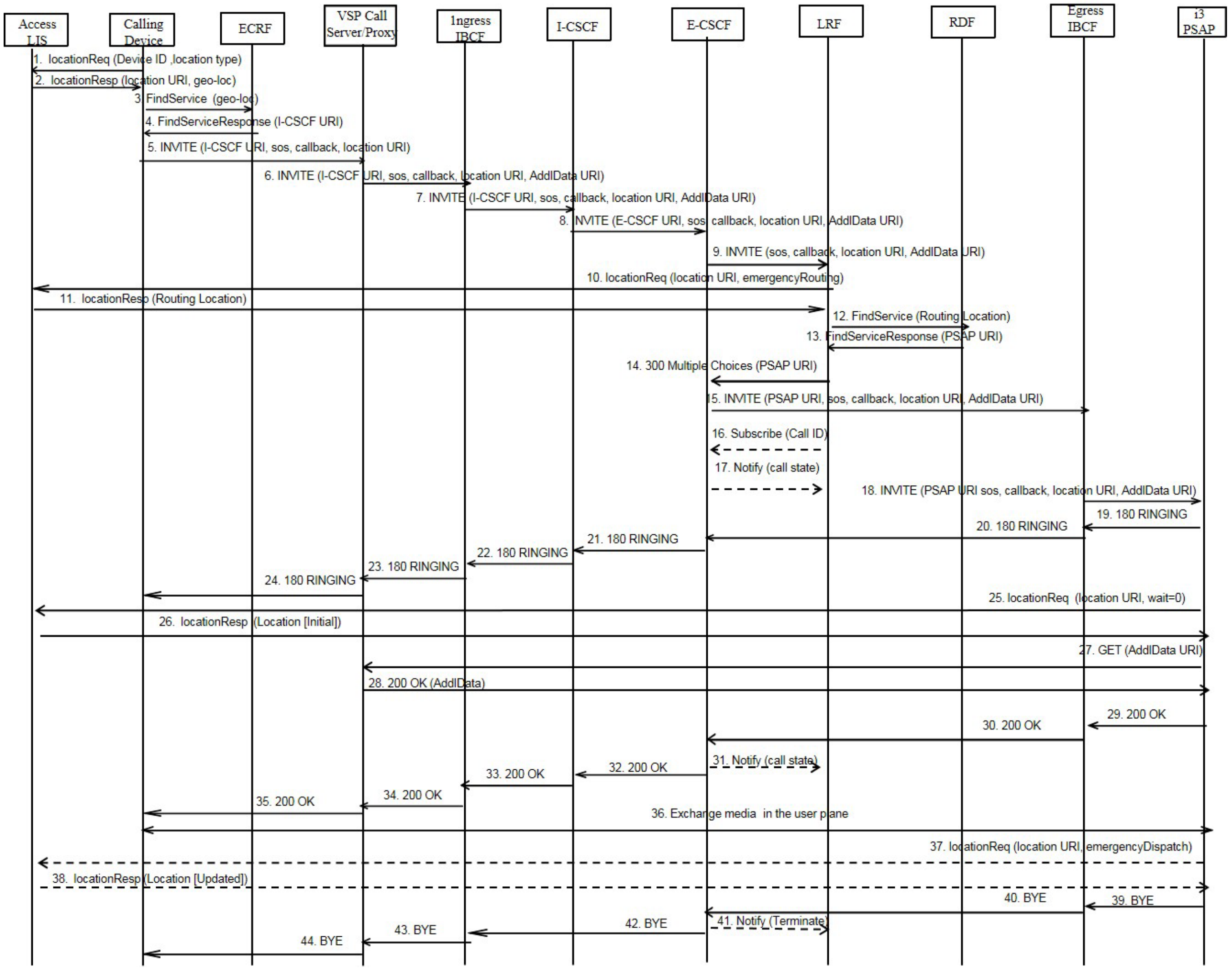

Access LIS
Calling Device
ECRF
VSP Call Server/Proxy
Ingress IBCF
I-CSCF
E-CSCF
LRF
RDF
Egress IBCF
i3 PSAP
1. locationReq (Device ID ,location type)
2. locationResp (location URI, geo-loc)
3 FindService (geo-loc)
4. FindServiceResponse (I-CSCF URI)
5. INVITE (I-CSCF URI, sos, callback, location URI)
6. INVITE (I-CSCF URI, sos, callback, location URI, AddlData URI)
7. INVITE (I-CSCF URI, sos, callback, location URI, AddlData URI)
8. INVITE (E-CSCF URI, sos, callback, location URI, AddlData URI)
9. INVITE (sos, callback, location URI, AddlData URI)
10. locationReq (location URI, emergencyRouting)
11. locationResp (Routing Location)
12. FindService (Routing Location)
13. FindServiceResponse (PSAP URI)
14. 300 Multiple Choices (PSAP URI)
15. INVITE (PSAP URI, sos, callback, location URI, AddlData URI)
16. Subscribe (Call ID)
17. Notify (call state)
18. INVITE (PSAP URI sos, callback, location URI, AddlData URI)
19. 180 RINGING
20. 180 RINGING
21. 180 RINGING
22. 180 RINGING
23. 180 RINGING
24. 180 RINGING
25. locationReq (location URI, wait=0)
26. locationResp (Location [Initial])
27. GET (AddlData URI)
28. 200 OK (AddlData)
29. 200 OK
30. 200 OK
31. Notify (call state)
32. 200 OK
33. 200 OK
34. 200 OK
35. 200 OK
36. Exchange media in the user plane
37. locationReq (location URI, emergencyDispatch)
38. locationResp (Location [Updated])
39. BYE
40. BYE
41. Notify (Terminate)
42. BYE
43. BYE
44. BYE

**Figure 8.13: Delivery of Non-IMS Emergency Call Origination to i3 PSAP with LbyR**

**Step 1.** Upon recognizing a request for emergency service, the calling device requests location by querying the LIS in the access network. (This example illustrates the use of the HELD protocol for the location request.) The locationRequest contains an identifier and appropriate credentials associated with the calling device, as well as an indication of the type of location being requested. In this example, the device requests geodetic location and a location URI. The locationRequest also includes a responseTime parameter (not shown) indicating how long the device is prepared to wait for a response or the purpose for which the device needs the location.

**Step 2.** The LIS responds to the location request by returning a geodetic location and a location URI.

**Step 3.** The device uses the geodetic location in the location response from the LIS and the emergency service URN (urn:service:sos) to query an ECRF for routing information.

**Step 4.** The ECRF responds by returning a URI associated with an I-CSCF in an IMS-based NG9-1-1 Emergency Services Network.

**Step 5.** The device generates a SIP INVITE message that includes a Route header that contains the I-CSCF URI, an emergency services service URN (urn:service:sos), callback information, and the location URI received from the LIS (along with a Geolocation-Routing header set to “yes”), and sends it to a Call Server/Proxy in its serving non-IMS originating network.

**Step 6.** The Call Server/Proxy adds Additional Data "by reference" to the received SIP INVITE message by including a Call-Info header that contains an Additional Data URI, and forwards the SIP INVITE message to an IBCF on the ingress side of the IMS-based NG9-1-1 Emergency Services Network.

**Step 7.** The (ingress) IBCF forwards the received INVITE message to the I-CSCF.

**Step 8.** The I-CSCF determines the address of the E-CSCF (based on provisioned data), and forwards the SIP INVITE message to it. The SIP INVITE message sent to the E-CSCF by the I-CSCF contains the E-CSCF URI in the Route header, and includes the callback information, "sos" service URN, location URI, and Additional Data URI, as received in the incoming SIP INVITE message.

**Step 9.** The E-CSCF forwards the SIP INVITE to the LRF.

**Step 10.** In this example, the SIP INVITE contains a location URI, so the LRF in the IMS-based NG9-1-1 Emergency Services Network queries a LIS in the access network (as identified in the location URI) for the routing location (i.e., responseTime parameter = emergencyRouting).

**Step 11.** The LIS returns the Routing Location that is associated with the location URI.

**Step 12.** The LRF queries the RDF using the location information obtained in Step 11.

**Step 13.** The RDF returns a Route URI. In this example, the Route URI is associated with an i3 PSAP that is served by the IMS-based NG9-1-1 Emergency Services Network.[23]

**Step 14.** The LRF redirects the call back to the E-CSCF, passing the Route (PSAP) URI.

**Step 15.** The E-CSCF generates an outgoing SIP INVITE message, using the information received from the LRF, as well as information received in the initial SIP INVITE message, and forwards it to the (egress) IBCF. The SIP INVITE message contains the PSAP URI in the Route header, the sos service URN in the Request-URI, the callback information in the From and P-Asserted-Identity headers, a Call-Info header containing an Additional Data URI, and the location URI in the Geolocation header. (A Geolocation-Routing header set to "yes" will also be present in the SIP INVITE message, as well as other SIP headers per RFC 3261 [Ref 18]).

**Step 16.** (Optional) The LRF may subscribe to the state of the call.

**Step 17.** (Conditional on Step 16) The E-CSCF sends an initial notification of the call state.

**Step 18.** The (egress) IBCF forwards the SIP INVITE message to the i3 PSAP with the callback information, Additional Data URI, and location URI received by the IMS-based NG9-1-1 Emergency Services Network in the SIP INVITE message from the non-IMS originating network.

**Step 19.** An indication that the call taker is being alerted is returned by the i3 PSAP to the (egress) IBCF (using a SIP 180 RINGING message).

**Step 20.** The (egress) IBCF passes the SIP 180 RINGING message to the E-CSCF.

**Step 21.** The E-CSCF passes the SIP 180 RINGING message to the I-CSCF.

**Step 22.** The I-CSCF passes the SIP 180 RINGING message to the (ingress) IBCF.

**Step 23.** The (ingress) IBCF passes the SIP 180 RINGING message to the Call Server/Proxy in the originating network.

**Step 24.** The Call Server/Proxy in the originating network passes the SIP 180 RINGING message to the calling device.

**Step 25.** Since the SIP INVITE message received by the i3 PSAP contains a location URI, the i3 PSAP queries the LIS in the access network (as identified in the location URI) for initial caller location

[23] If policy associated with the Route URI returned by the RDF requires that the LRF obtain Additional Data, the LRF will also have to de-reference with the Call Server/Proxy in the originating network to obtain Additional Data "by value". This example assumes that the LRF does not need to obtain Additional Data to determine the destination PSAP for the call.

(i.e., responseTime contains a wait timer value of “0”). (Note that this can occur any time after Step18.)

**Step 26.** The LIS supplies the initial caller location information to the PSAP. The initial display location information is displayed at the PSAP CPE.

**Step 27.** Since the SIP INVITE message received by the i3 PSAP also contains an Additional Data URI, the i3 PSAP queries the Call Server/Proxy in the originating network (or Additional Data Repository [ADR] associated with it), as identified in the Additional Data URI for Additional Data using a GET request. (Note that this can occur any time after Step18.)

**Step 28.** The Call Server/ADR returns Additional Data (by value) to the i3 PSAP.

**Step 29.** When the i3 PSAP answers the call, it returns a SIP 200 OK message to the (egress) IBCF.

**Step 30.** The (egress) IBCF passes the SIP 200 OK message to the E-CSCF.

**Step 31.** (Conditional on Step 16) The E-CSCF sends a notification to the LRF updating the call state.

**Step 32.** The E-CSCF passes the SIP 200 OK message to the I-CSCF.

**Step 33.** The I-CSCF passes the SIP 200 OK message to the (ingress) IBCF.

**Step 34.** The (ingress) IBCF passes the SIP 200 OK message to the Call Server/Proxy in the originating network.

**Step 35.** The Call Server/Proxy passes the SIP 200 OK message to the calling device.

**Step 36.** At this point a two-way connection is established between the caller and the PSAP.

**Step 37.** (Optional) The PSAP queries the LIS in the access network (as identified in the location URI) for updated (dispatch) location information (responseTime parameter = “emergencyDispatch” in this example).

**Step 38.** (Conditional on Step 37) The LIS in the access network supplies the updated (dispatch) location to the i3 PSAP and it is displayed on the PSAP CPE.

**Step 39.** At some point the call is terminated. In this call flow, the i3 PSAP terminates the call and sends a SIP BYE message to the (egress) IBCF.

**Step 40.** The SIP BYE is passed from the (egress) IBCF to the E-CSCF.

**Step 41.** (Conditional on Step 16) The E-CSCF then notifies the LRF that the call has terminated.

**Step 42.** The E-CSCF passes the SIP BYE message to the (ingress) IBCF.

**Step 43.** The (ingress) IBCF passes the SIP BYE message to the Call Server/Proxy in the originating network.

**Step 44.** The Call Server/Proxy passes the SIP BYE message to the calling device.

### 8.6.2 Delivery of Emergency Call Origination from Non-IMS Origination Network to Legacy PSAP with LbyR

The call flow provided in Figure 8-14 illustrates a scenario where an emergency call is delivered by a non-IMS i3-compliant VoIP origination network to an IMS-based NG9-1-1 Emergency Services Network with LbyR. Upon detecting an emergency origination, the calling device requests location by querying a Location Information Server (LIS) in the access network, using the HELD protocol. The HELD locationRequest contains an identifier associated with the calling device and appropriate credentials. It also contains an indication of the form that the provided location information should take. In this example call flow, the device requests geodetic location and a location URI. The LIS responds with geodetic location information and a location URI. The device uses the geodetic location returned in the HELD locationResponse to query an Emergency Call Routing Function (ECRF) for routing information. The ECRF returns a URI associated with the I-CSCF in an IMS-based NG9-1-1 Emergency Services Network. The device forwards the emergency session request to a Call Server/Proxy in its serving non-IMS, i3-compliant originating network. The SIP INVITE message signaled by the device to the Call Server/Proxy includes a Route header that contains the URI of an I-CSCF in the IMS-based NG9-1-1 Emergency Services Network, an emergency services service URN (urn:service:sos) in the Request-URI, callback information in the P-Asserted-Identity header, and a LbyR URI in the Geolocation header. (A Geolocation-Routing header set to “yes”, and other SIP headers will also be included in the SIP INVITE message, but are not specifically illustrated in Figure 8-14.) The Call Server/Proxy forwards the SIP INVITE to an IBCF on the ingress side of the IMS-based NG9-1-1 Emergency Services Network. The IBCF forwards the SIP INVITE to the I-CSCF and the I-CSCF forwards the SIP INVITE message to the (pre-configured) E-CSCF, populating the E-CSCF URI in the Route header. The E-CSCF forwards the SIP INVITE to the LRF. The LRF de-references the received location URI by sending a de-reference request to the LIS in the access network. The LRF then uses the LbyV received in the de-reference response to query the RDF. In this example call flow, the Route URI that is returned by the RDF is associated with a legacy PSAP. The call flow depicted in Figure 8-14 assumes that the call is forwarded by the E-CSCF to the LPG via an egress IBCF. The LPG may generate a 7/10-digit pANI for the call and, based on per-PSAP provisioning, associates an appropriate Numbering Plan Digit (NPD) or ANI II value with the call (depending on whether the PSAP supports a Traditional MF interface or an Enhanced MF interface).

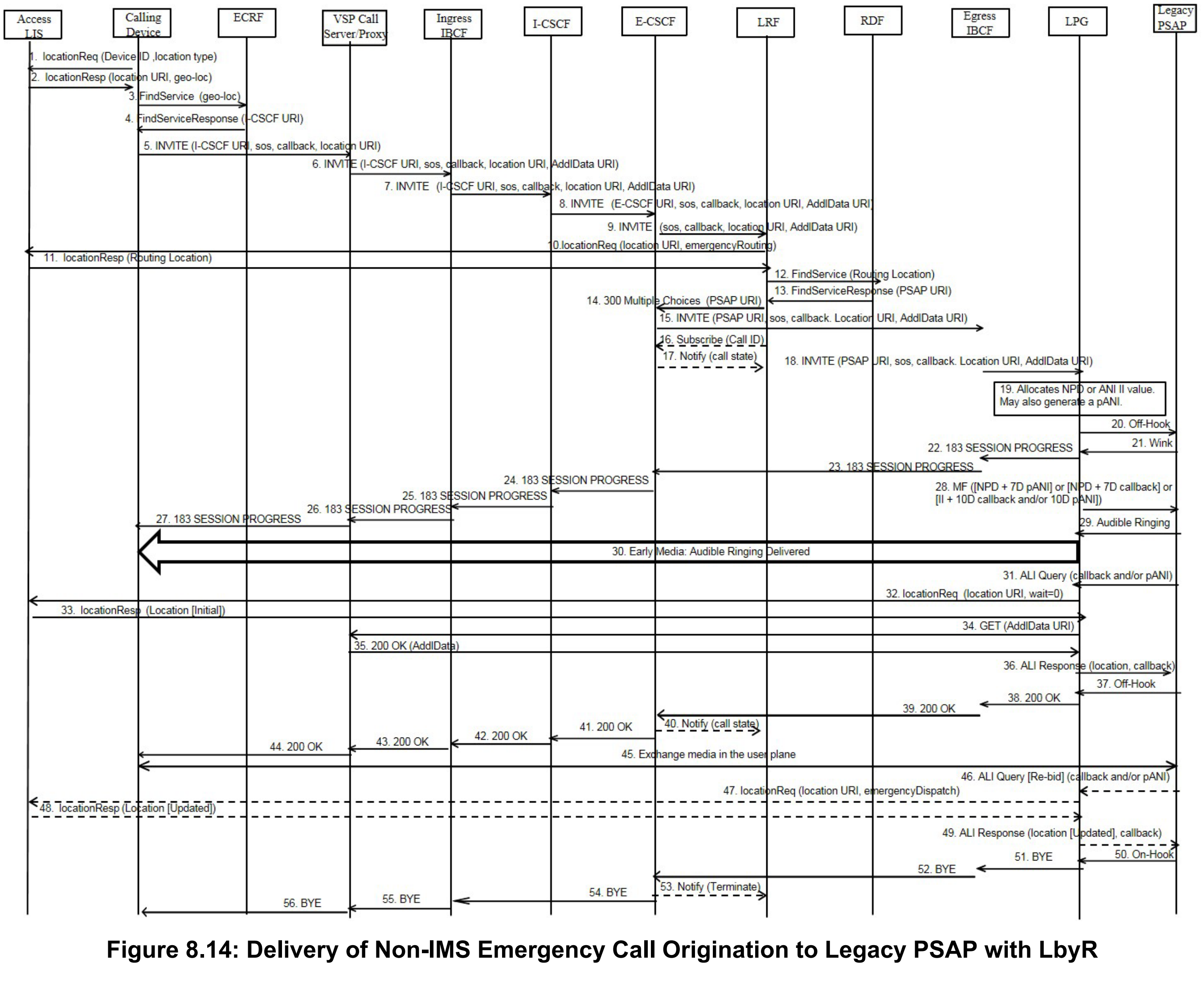

Access LIS
Calling Device
ECRF
VSP Call Server/Proxy
Ingress IBCF
I-CSCF
E-CSCF
LRF
RDF
Egress IBCF
LPG
Legacy PSAP
1. locationReq (Device ID ,location type)
2. locationResp (location URI, geo-loc)
3. FindService (geo-loc)
4. FindServiceResponse (I-CSCF URI)
5. INVITE (I-CSCF URI, sos, callback, location URI)
6. INVITE (I-CSCF URI, sos, callback, location URI, AddlData URI)
7. INVITE (I-CSCF URI, sos, callback, location URI, AddlData URI)
8. INVITE (E-CSCF URI, sos, callback, location URI, AddlData URI)
9. INVITE (sos, callback, location URI, AddlData URI)
10.locationReq (location URI, emergencyRouting)
11. locationResp (Routing Location)
12. FindService (Routing Location)
13. FindServiceResponse (PSAP URI)
14. 300 Multiple Choices (PSAP URI)
15. INVITE (PSAP URI, sos, callback. Location URI, AddlData URI)
16. Subscribe (Call ID)
17. Notify (call state)
18. INVITE (PSAP URI, sos, callback. Location URI, AddlData URI)
19. Allocates NPD or ANI II value. May also generate a pANI.
20. Off-Hook
21. Wink
22. 183 SESSION PROGRESS
23. 183 SESSION PROGRESS
24. 183 SESSION PROGRESS
25. 183 SESSION PROGRESS
26. 183 SESSION PROGRESS
27. 183 SESSION PROGRESS
28. MF ([NPD + 7D pANI] or [NPD + 7D callback] or [II + 10D callback and/or 10D pANI])
29. Audible Ringing
30. Early Media: Audible Ringing Delivered
31. ALI Query (callback and/or pANI)
32. locationReq (location URI, wait=0)
33. locationResp (Location [Initial])
34. GET (AddlData URI)
35. 200 OK (AddlData)
36. ALI Response (location, callback)
37. Off-Hook
38. 200 OK
39. 200 OK
40. Notify (call state)
41. 200 OK
42. 200 OK
43. 200 OK
44. 200 OK
45. Exchange media in the user plane
46. ALI Query [Re-bid] (callback and/or pANI)
47. locationReq (location URI, emergencyDispatch)
48. locationResp (Location [Updated])
49. ALI Response (location [Updated], callback)
50. On-Hook
51. BYE
52. BYE
53. Notify (Terminate)
54. BYE
55. BYE
56. BYE

**Figure 8.14: Delivery of Non-IMS Emergency Call Origination to Legacy PSAP with LbyR**

**Step 1.** Upon recognizing a request for emergency service, the calling device requests location by querying the LIS in the access network. (This example illustrates the use of the HELD protocol for the location request.) The locationRequest contains an identifier and appropriate credentials associated with the calling device, as well as an indication of the type of location being requested. In this example, the device requests geodetic location and a location URI. The locationRequest also includes a responseTime parameter (not shown) indicating how long the device is prepared to wait for a response or the purpose for which the device needs the location.

**Step 2.** The LIS responds to the location request by returning a geodetic location and a location URI.

**Step 3.** The device uses the geodetic location in the location response from the LIS and the emergency service URN (urn:service:sos) to query an ECRF for routing information.

**Step 4.** The ECRF responds by returning a URI associated with an I-CSCF in an IMS-based NG9-1-1 Emergency Services Network.

**Step 5.** The device generates a SIP INVITE message that includes a Route header that contains the I-CSCF URI, an emergency services service URN (urn:service:sos), callback information, and the location URI received from the LIS, and sends it to a Call Server/Proxy in its serving non-IMS originating network.

**Step 6.** The Call Server/Proxy adds Additional Data (by reference) to the received SIP INVITE message by including a Call-Info header that contains an Additional Data URI and forwards the SIP INVITE message to an IBCF on the ingress side of the IMS-based NG9-1-1 Emergency Services Network.

**Step 7.** The (ingress) IBCF forwards the received INVITE message to the I-CSCF.

**Step 8.** The I-CSCF determines the address of the E-CSCF (based on provisioned data) and forwards the SIP INVITE message to the E-CSCF. The SIP INVITE message sent to the E-CSCF by the I-CSCF contains the E-CSCF URI in the Route header, and includes the callback information, “sos” service URN, location URI, and Additional Data (by reference) as received in the incoming SIP INVITE message.

**Step 9.** The E-CSCF forwards the SIP INVITE to the LRF.

**Step 10.** In this example, the SIP INVITE contains a LbyR URI, so the LRF in the IMS-based NG9-1-1 Emergency Services Network queries the LIS in the access network (as identified in the location URI) for routing location (i.e., responseTime parameter = emergencyRouting).

**Step 11.** The LIS returns the Routing Location that is associated with the location URI.

**Step 12.** The LRF queries the RDF using the location information obtained in Step 11 and the emergency service URN (urn:service:sos).

**Step 13.** The RDF returns a Route URI. In this example, the Route URI is associated with a legacy PSAP that is served by the IMS-based NG9-1-1 Emergency Services Network.

**Step 14.** The LRF redirects the call back to the E-CSCF, passing the Route (PSAP) URI.[24]

**Step 15.** The E-CSCF generates an outgoing SIP INVITE message, using the information received from the LRF, as well as information received in the initial SIP INVITE message, and forwards it to the (egress) IBCF. The SIP INVITE message includes the PSAP URI in the Route header, the sos service URN in the Request-URI, the callback information in the From and P-Asserted-Identity headers, the LbyR URI in the Geolocation header, and an Additional Data URI in the Call-Info header. (A Geolocation-Routing header set to “yes” will also be present in the SIP INVITE message, as well as other SIP headers per RFC 3261 [Ref 18]).

**Step 16.** (Optional) The LRF may subscribe to the state of the call.

**Step 17.** (Conditional on Step 16) The E-CSCF sends an initial notification of the call state.

**Step 18.** The (egress) IBCF forwards the SIP INVITE to the LPG.

[24] If policy associated with the Route URI returned by the RDF requires that the LRF obtain Additional Data, the LRF will also have to de-reference with the Call Server/Proxy in the originating network to obtain Additional Data “by value”. This example assumes that the LRF does not need to obtain Additional Data to determine the destination PSAP for the call.

**Step 19.** The LPG determines, based on provisioning, whether the PSAP associated with the received PSAP URI supports a Traditional MF or Enhanced MF interface. Depending on the type of interface supported by the PSAP, the LPG may generate a pANI and will assign an appropriate NPD or ANI II value to the call, following the procedures specified in Clause 6.2.2 of NENA-STA-010.3 [Ref 27].

**Step 20.** The LPG generates an off-hook signal toward the legacy PSAP.

**Step 21.** The legacy PSAP returns a wink signal back to the LPG.

**Step 22.** The LPG generates a 183 Session Progress message and sends it to the (egress) IBCF.

**Step 23.** The (egress) IBCF passes the 183 Session Progress message to the E-CSCF.

**Step 24.** The E-CSCF passes the 183 Session Progress message to the I-CSCF.

**Step 25.** The I-CSCF passes the 183 Session Progress message to the (ingress) IBCF.

**Step 26.** The (ingress) IBCF passes the SIP 183 Session Progress message to the Call Server/Proxy in the originating network.

**Step 27.** The Call Server/Proxy passes the SIP 183 Session Progress message to the calling device.

**Step 28.** The LPG delivers the call to the legacy PSAP, mapping the SIP signaling from the incoming INVITE message to the outgoing Traditional or Enhanced MF signaling sequences, as described below:

- For PSAPs that support a Traditional MF interface where delivery of callback information is preferred, the LPG will map the information received in the From/P-Asserted-Identity headers of the incoming SIP INVITE message, if that information is in the form of (or easily converted to) a 10-digit NANP number with an appropriate NPA value. If the callback information is not in the form of (or easily converted to) a 10-digit NANP number, the LPG will populate the pANI generated in Step 19 in the outgoing MF signaling sequence. The outgoing signaling will also include the NPD value obtained in Step 19. The LPG will signal the NPD and 7-digit callback number or pANI in the MF ANI sequence KP + NPD + NXX XXXX + ST.
- For PSAPs that support a Traditional MF interface where delivery of location information is preferred, the LPG will populate the pANI generated in Step 19, along with an appropriate NPD digit (i.e., NPD + 7D pANI) in the MF ANI sequence KP + NPD + NXX XXXX + ST.
- For PSAPs that support an Enhanced MF interface with 10-digit delivery where delivery of callback information is preferred, the LPG will map the information received in the From/P-Asserted-Identity headers of the SIP INVITE message, if that information is in the form of (or easily converted to) a 10-digit NANP number with an appropriate NPA. If the callback information is not in the form of (or easily converted to) a 10-digit NANP number, the LPG will signal the pANI, generated in Step 19 in the outgoing MF signaling sequence. The LPG will signal the II digits derived in Step 19 plus the 10D pANI or 10D callback number to the PSAP in the MF ANI sequence KP + II + NPA NXX XXXX + ST´.
- For PSAPs that support an Enhanced MF interface with 10-digit delivery where delivery of location information is preferred, the LPG will populate the pANI it generated in Step 19, along with an appropriate II value (i.e., II digits plus the 10D pANI), in the MF ANI sequence KP + II + NPA NXX XXXX + ST´.
- For PSAPs that support an Enhanced MF interface with 20-digit delivery, the LPG will populate the pANI (associated with the location information) that it generated in Step 19 and the callback information that it received in the From/PAI headers (or a pANI if the callback information is not in the form of, or easily converted to, a 10-digit NANP number), along with the II value allocated by the LPG in Step 19, to the MF sequence KP + II + NPA NXX XXXX + ST + KP + NPA NXX XXXX + ST, where the first 10-digit number is associated with the callback information from the PAI/From headers and the second 10-digit number contains the pANI associated with the location.

**Step 29.** Audible ringing is returned by the legacy PSAP to the LPG.

**Step 30.** Audible ringing is passed to the originating device/caller.

**Step 31.** The legacy PSAP sends a location query to the LPG using a legacy ALI protocol. The ALI query includes the 10-digit callback information and/or the pANI received in Step 28. (Note that this can happen any time after Step 28.)

**Step 32.** The LPG sends a de-reference request to the LIS in the access network (as identified in the location URI associated with the pANI/callback information) for initial caller location (i.e., responseTime contains a wait timer value of "0").

**Step 33.** The LIS supplies the initial caller location information to the LPG in the de-reference response.

**Step 34.** In this example, the SIP INVITE received by the LPG contains an Additional Data URI, so the LPG queries the Call Server/Proxy (as identified in the URI) for Additional Data using an HTTPS GET operation.

**Step 35.** The Call Server/Proxy provides the requested Additional Data in a 200 OK response.[25]

**Step 36.** The LPG returns an ALI response to the legacy PSAP that includes the initial caller location information, a callback number and other information (e.g., class of service), as appropriate for the interface.

**Step 37.** When the PSAP answers the call, it returns an off-hook signal to the LPG.

**Step 38.** In response to the off-hook signal, the LPG generates a SIP 200 OK message and passes it to the (egress) IBCF.

**Step 39.** The (egress) IBCF passes the SIP 200 OK message to the E-CSCF.

**Step 40.** (Conditional on Step 17) The E-CSCF sends a notification to the LRF updating the call state.

**Step 41.** The E-CSCF passes the SIP 200 OK message to the I-CSCF.

**Step 42.** The I-CSCF passes the SIP 200 OK message to the (ingress) IBCF.

**Step 43.** The (ingress) IBCF passes the SIP 200 OK message to the Call Server/Proxy in the originating network.

**Step 44.** The Call Server/Proxy passes the SIP 200 OK message to the calling device.

**Step 45.** At this point a two-way connection is established between the caller and the PSAP.

**Step 46.** (Optional) The legacy PSAP sends an ALI re-bid query (containing the callback information and/or pANI received in Step 28) to the LPG.

**Step 47.** (Optional) The LPG queries the LIS in the access network (as identified in the location URI that is associated with the pANI/callback information) for updated (dispatch) location information (responseTime parameter = "emergencyDispatch" in this example).

**Step 48.** (Conditional on Step 47) The LIS in the access network supplies updated (dispatch) location to the LPG.

**Step 49.** (Conditional on Step 46) The LPG supplies updated (dispatch) location (along with callback and other non-location information, as appropriate for the interface) for display at the legacy PSAP.

**Step 50.** At some point the call is terminated. In this call flow, the PSAP terminates the call and sends an on-hook indication to the LPG.

**Step 51.** The LPG maps the on-hook indication to a SIP BYE message and sends the SIP BYE message to the (egress) IBCF.

[25] Note that Steps 32 through 35 can happen any time after Step 28, and that Steps 32 and 33 can be performed either before or after Steps 34 and 35.

**Step 52.** The (egress) IBCF passes the SIP BYE message to the E-CSCF.

**Step 53.** (Conditional on Step 16) The E-CSCF then notifies the LRF that the call has terminated.

**Step 54.** The E-CSCF passes the SIP BYE message to the (ingress) IBCF.

**Step 55.** The (ingress) IBCF passes the SIP BYE message to the Call Server/Proxy in the originating network.

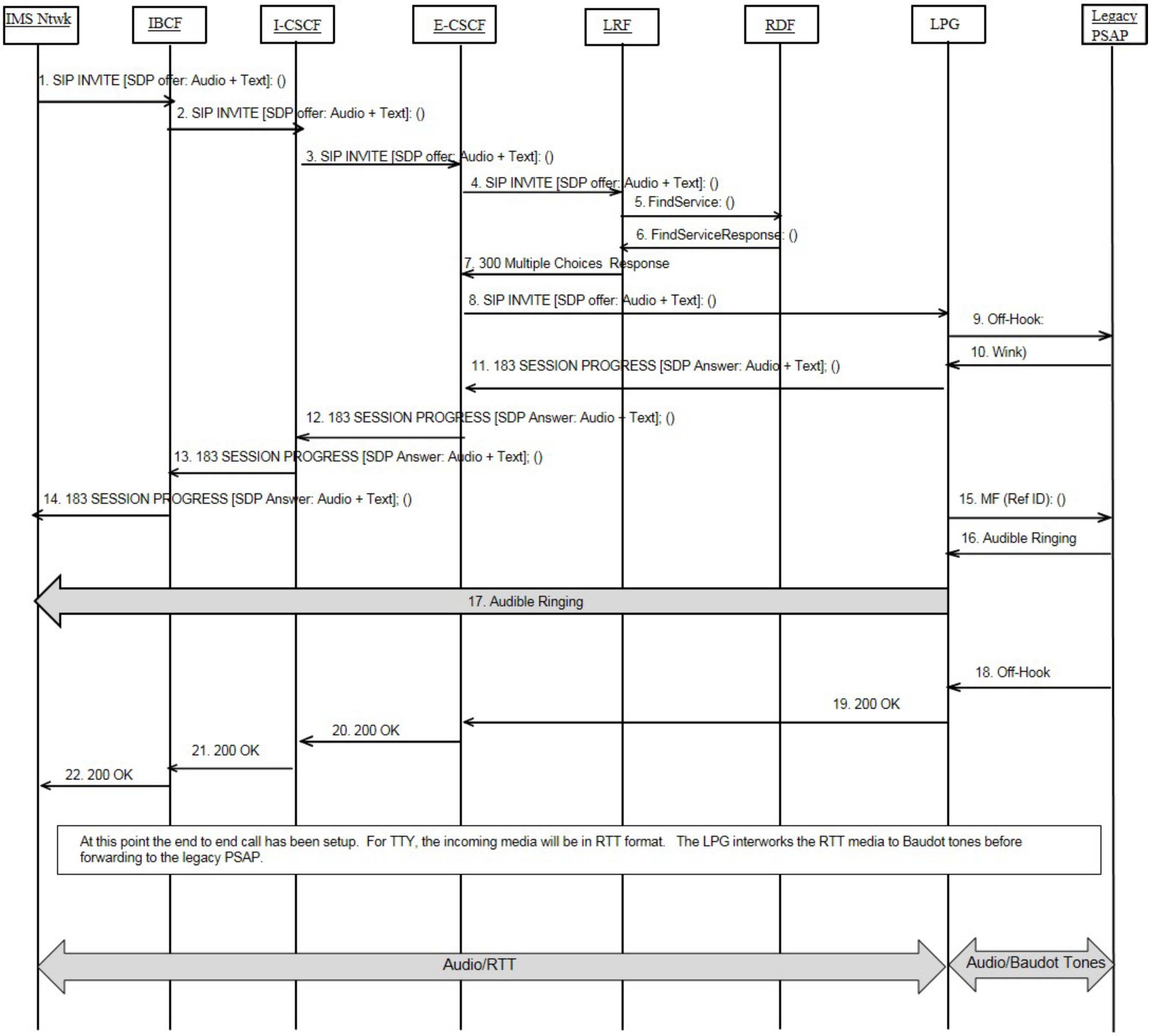
**Step 56.** The Call Server/Proxy passes the SIP BYE message to the calling device.

## *8.7 TTY Interworking on Emergency Calls to Legacy/i3 PSAPs*

### 8.7.1 RTT Calls from IMS Originating Network to Legacy PSAP via NG9-1-1

This call flow illustrates a scenario where an incoming RTT call from an IMS originating network is delivered via an IMS-based NG9-1-1 Emergency Services Network to a legacy PSAP as a TTY call. This call flow shows an incoming emergency call delivered to an IMS-based NG9-1-1 Emergency Services Network with audio and text media included in the SDP offer and LbyV.

NOTE: The PRACK messages are not shown for simplicity.


IMS Ntwk
IBCF
I-CSCF
E-CSCF
LRF
RDF
LPG
Legacy PSAP
1. SIP INVITE [SDP offer: Audio + Text]: ()
2. SIP INVITE [SDP offer: Audio + Text]: ()
3. SIP INVITE [SDP offer: Audio + Text]: ()
4. SIP INVITE [SDP offer: Audio + Text]: ()
5. FindService: ()
6. FindServiceResponse: ()
7. 300 Multiple Choices Response
8. SIP INVITE [SDP offer: Audio + Text]: ()
9. Off-Hook:
10. Wink)
11. 183 SESSION PROGRESS [SDP Answer: Audio + Text]; ()
12. 183 SESSION PROGRESS [SDP Answer: Audio + Text]; ()
13. 183 SESSION PROGRESS [SDP Answer: Audio + Text]; ()
14. 183 SESSION PROGRESS [SDP Answer: Audio + Text]; ()
15. MF (Ref ID): ()
16. Audible Ringing
17. Audible Ringing
18. Off-Hook
19. 200 OK
20. 200 OK
21. 200 OK
22. 200 OK
Audio/RTT
Audio/Baudot Tones

At this point the end to end call has been setup. For TTY, the incoming media will be in RTT format. The LPG interworks the RTT media to Baudot tones before forwarding to the legacy PSAP.

**Figure 8.15: RTT Calls from IMS Originating Network to Legacy PSAP via NG9-1-1**

**Step 1.** The IBCF in the IMS originating network sends an emergency call origination (i.e., a SIP INVITE) to the (ingress) IBCF in the NG9-1-1 network with an SDP offer of audio and RFC 4103 [Ref 29] text media to be set up. The SIP INVITE also contains a media feature tag value of “text”.

**Step 2.** The IBCF forwards the SIP INVITE to the I-CSCF.

**Step 3.** The I-CSCF forwards the SIP INVITE to the pre-configured E-CSCF.

**Step 4.** The E-CSCF forwards the SIP INVITE to the LRF.

**Step 5.** The LRF queries the RDF using the location information received in the body of the received SIP INVITE message.

**Step 6.** The RDF returns a Route URI. In this example, the Route URI is associated with a legacy PSAP that is served by the IMS-based NG9-1-1 Emergency Services Network.

**Step 7.** The LRF redirects the call back to the E-CSCF, passing the Route (PSAP) URI in 300 Multiple Choices response.

**Step 8.** The E-CSCF generates an outgoing SIP INVITE message, using the information received from the LRF as well as information received in the initial SIP INVITE message, and forwards it to the LPG.

**Step 9.** The LPG generates an Off Hook MF signal and forwards it to the legacy PSAP.

**Step 10.** The legacy PSAP returns a wink signal back to LPG.

**Step 11.** The LPG generates a SIP: 183 SESSION PROGRESS message (with an SDP Answer) back to E-CSCF. The Contact header field in the SIP 183 SESSION PROGRESS message sent by the LPG to the E-CSCF shall include a "urn:nena:media-feature.TTY-interworking" media feature tag.

**Step 12.** The E-CSCF forwards the SIP: 183 SESSION PROGRESS message to I-CSCF.

**Step 13.** The I-CSCF forwards the SIP: 183 SESSION PROGRESS message to the NG9-1-1 IBCF.

**Step 14.** The NG9-1-1 IBCF forwards the SIP 183 SESSION PROGRESS message to the IBCF of the originating IMS network.

**Step 15.** The LPG delivers the call to the legacy PSAP, mapping the SIP signaling from the incoming INVITE message to the outgoing Traditional or Enhanced MF signaling sequences.

**Step 16.** The legacy PSAP delivers Audible Ringing to LPG.

**Step 17.** The LPG delivers the Audible Ringing tone as early media to the originating network.

**Step 18.** When the PSAP answers the call, it returns an off-hook signal back to the LPG.

**Step 19.** In response to the off-hook signal, the LPG generates a SIP 200 OK message and passes it to the E-CSCF.

**Step 20.** The E-CSCF passes the SIP 200 OK message to the I-CSCF.

**Step 21.** The I-CSCF passes the SIP 200 OK message to the NG9-1-1 IBCF.

**Step 22.** The NG9-1-1 IBCF passes the SIP 200 OK message to the IMS originating network IBCF.

Once an emergency TTY call is set up, the incoming audio and RFC 4103 [Ref 29] text media from the IMS originating network is forwarded to the LPG. The LPG, upon detecting the text media type, converts the RTT (RFC 4103 [Ref 29]) text media to Baudot tones before forwarding the data to the legacy PSAP. If the LPG receives simultaneous RFC 4103 [Ref 29] text and audio media associated with an emergency call (or one media type is added to an existing session involving the other media type), and since the audio media may include Baudot tones or other audio sounds, the LPG must notch the audio frequencies used for Baudot tones from the received audio media and then insert the Baudot tones transcoded from the received RFC 4103 [Ref 29] text to minimize the distortion of the Baudot tones delivered to the PSAP. See Clause 6.2 of NENA-STA-010.3 [Ref 27] for further details regarding RTT-TTY interworking at an LPG.

### 8.7.2 TTY Calls from Legacy Originating Network to an i3 PSAP via NG9-1-1

This call flow illustrates a TTY emergency call originating in a legacy circuit switched network and terminated at an i3 PSAP. An i3 LNG handles a TTY emergency origination by first establishing an audio session with the PSAP and subsequently requesting, or processing an incoming request for, the addition of an RFC 4103 [Ref 29] text media session as described below.

If the emergency call is delivered to the PSAP as a "silent" call, the LNG must be capable of receiving and processing a re-INVITE from an i3 PSAP or LPG that requests the addition of RFC 4103 [Ref 29] text media to the existing emergency session.

If the LNG detects Baudot tones from the caller after an audio session is established, and an RFC 4103 [Ref 29] text media session has not already been established (via a re-INVITE from an i3 PSAP or LPG), the LNG shall generate a SIP re-INVITE message that includes an offer in the SDP describing a media format associated with real-time text (as specified in RFC 4103 [Ref 29]), and send the SIP re-INVITE message to the ingress IBCF. The LNG will buffer any real-time text that is converted from the received Baudot tones until such time as the real-time text media session is established (i.e., a 200 OK message is received from the NIF component in response to the re-INVITE) and the real-time text can be passed forward.

If the LNG detects Baudot tones from the caller before an audio session is established, the LNG shall wait for the audio session to be established, and if a text session has not already been established, the LNG shall generate a SIP re-INVITE message that includes an offer in the SDP describing a media format associated with real-time text (as specified in RFC 4103 [Ref 29]), and send the SIP re-INVITE message to the IBCF. The LNG will buffer any real-time text that is converted from the received Baudot tones until such time as the real-time text media session is established (i.e., a 200 OK message is received from the NIF component in response to the re-INVITE) and the real-time text can be passed forward. See Clause 6.1 of NENA-STA-010.3 [Ref 27] for further details regarding RTT-TTY interworking at an i3 LNG.

Part I of the call flow example illustrated below shows the i3 LNG setting up the call with an SDP offer of Audio media in the initial SIP INVITE message. Part II of the call flow shows the i3 LNG generating a re-INVITE to request the addition of a real-time text media session to the call upon detecting Baudot tones from the caller. The call flow assumes LbyV.

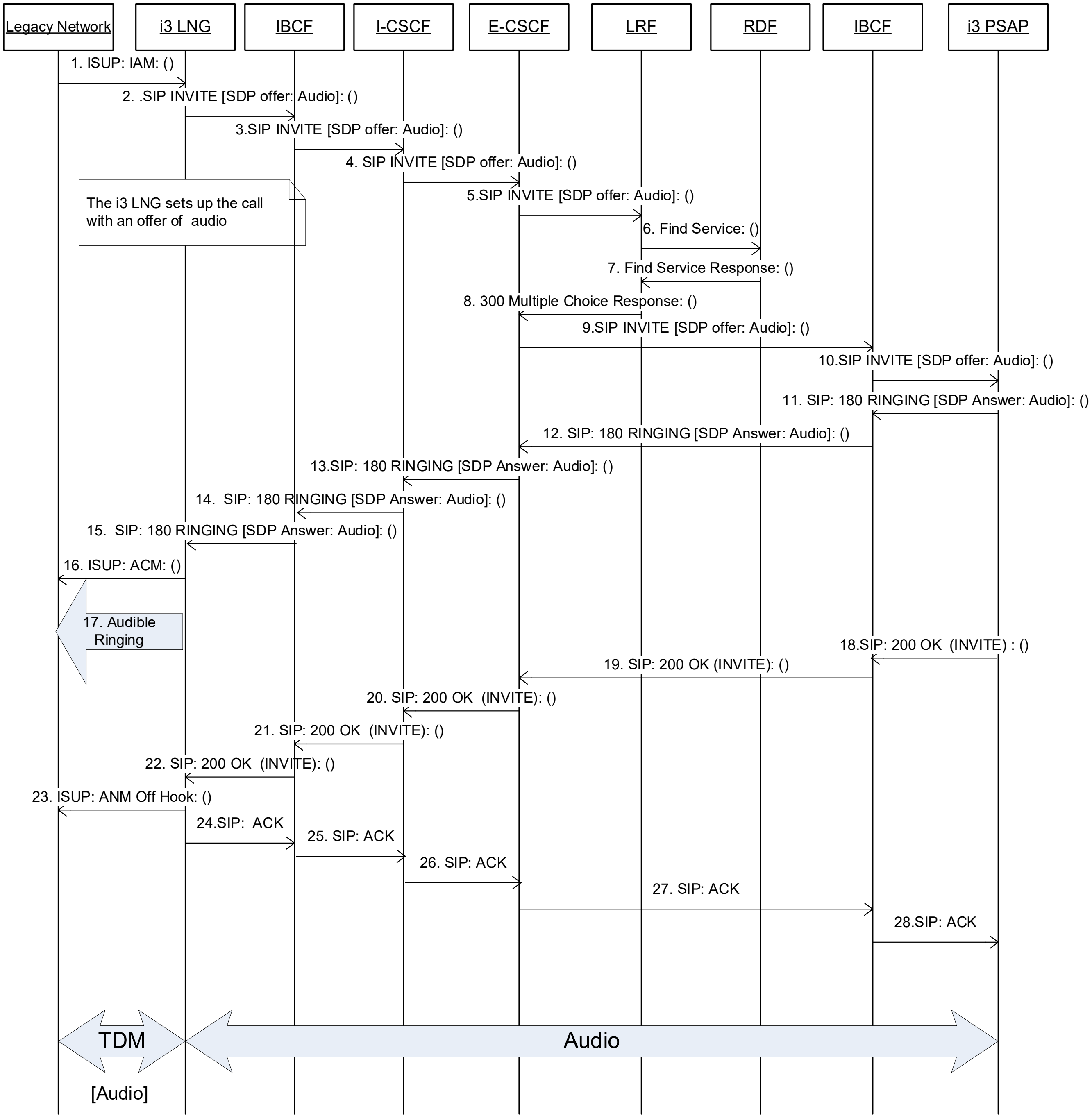

Legacy Network
i3 LNG
IBCF
I-CSCF
E-CSCF
LRF
RDF
IBCF
i3 PSAP
1. ISUP: IAM: ()
2. .SIP INVITE [SDP offer: Audio]: ()
3.SIP INVITE [SDP offer: Audio]: ()
4. SIP INVITE [SDP offer: Audio]: ()
The i3 LNG sets up the call with an offer of audio
5.SIP INVITE [SDP offer: Audio]: ()
6. Find Service: ()
7. Find Service Response: ()
8. 300 Multiple Choice Response: ()
9.SIP INVITE [SDP offer: Audio]: ()
10.SIP INVITE [SDP offer: Audio]: ()
11. SIP: 180 RINGING [SDP Answer: Audio]: ()
12. SIP: 180 RINGING [SDP Answer: Audio]: ()
13.SIP: 180 RINGING [SDP Answer: Audio]: ()
14. SIP: 180 RINGING [SDP Answer: Audio]: ()
15. SIP: 180 RINGING [SDP Answer: Audio]: ()
16. ISUP: ACM: ()
17. Audible Ringing
18.SIP: 200 OK (INVITE) : ()
19. SIP: 200 OK (INVITE): ()
20. SIP: 200 OK (INVITE): ()
21. SIP: 200 OK (INVITE): ()
22. SIP: 200 OK (INVITE): ()
23. ISUP: ANM Off Hook: ()
24.SIP: ACK
25. SIP: ACK
26. SIP: ACK
27. SIP: ACK
28.SIP: ACK
TDM
[Audio]
Audio

**Figure 8.16: TTY Calls from Legacy Originating Network to an i3 PSAP via NG9-1-1 – Part I**

**Step 1.** The i3 LNG receives an SS7 IAM message from the legacy network.

**Step 2.** The i3 LNG translates the message into a SIP INVITE message with SDP offer of Audio media and a media feature tag with the value “urn:nena:media-feature.TTY-interworking”, and sends the SIP INVITE message towards the IBCF.

**Step 3.** The IBCF forwards the SIP INVITE to the I-CSCF.

**Step 4.** The I-CSCF forwards the SIP INVITE to the pre-configured E-CSCF.

**Step 5.** The E-CSCF forwards the SIP INVITE to the LRF.

**Step 6.** The LRF queries the RDF using the location information received in the body of the received SIP INVITE message.

**Step 7.** The RDF returns a Route URI. In this example, the Route URI is associated with an i3 PSAP that is served by the IMS-based NG9-1-1 Emergency Services Network.

**Step 8.** The LRF redirects the call back to the E-CSCF, passing the Route (PSAP) URI in 300 Multiple Choices response.

**Step 9.** The E-CSCF generates an outgoing SIP INVITE message, using the information received from the LRF as well as information received in the initial SIP INVITE message, and forwards it to the (egress) IBCF.

**Step 10.** The IBCF forwards the INVITE to the i3 PSAP.

**Step 11.** The i3 PSAP sends a SIP: 180 RINGING message with [SDP Answer: Audio] that includes a media feature tag of “text” to IBCF.

**Step 12.** The IBCF forwards the SIP: 180 RINGING message back to E-CSCF.

**Step 13.** The E-CSCF forwards the SIP: 180 RINGING message to I-CSCF.

**Step 14.** The I-CSCF forwards the SIP: 180 RINGING message to the IBCF.

**Step 15.** The IBCF forwards the SIP: 180 RINGING message to the i3 LNG.

**Step 16.** The i3 LNG interworks the SIP: 180 RINGING message to an SS7 ACM indication towards the legacy network.

**Step 17.** The i3 LNG generates Audible Ringing towards legacy network.

**Step 18.** When the PSAP answers the call, it returns a SIP: 200 OK message to the (egress) IBCF.

**Step 19.** The IBCF forwards the SIP: 200 OK message to E-CSCF.

**Step 20.** The E-CSCF passes the SIP: 200 OK message to the I-CSCF.

**Step 21.** The I-CSCF passed the SIP: 200 OK message to IBCF.

**Step 22.** The IBCF passes the SIP: 200 OK message to the i3 LNG.

**Step 23.** The i3 LNG interworks the SIP: 200 OK message to an SS7 ANM message towards the legacy network.

**Step 24.** The i3 LNG returns an ACK to the IBCF in response to the SIP: 200 OK message.

**Step 25.** The IBCF passes the ACK to the I-CSCF.

**Step 26.** The I-CSCF passes the ACK to the E-CSCF.

**Step 27.** The E-CSCF passes the ACK to (egress) IBCF.

**Step 28.** The IBCF passes the ACK to the i3 PSAP.

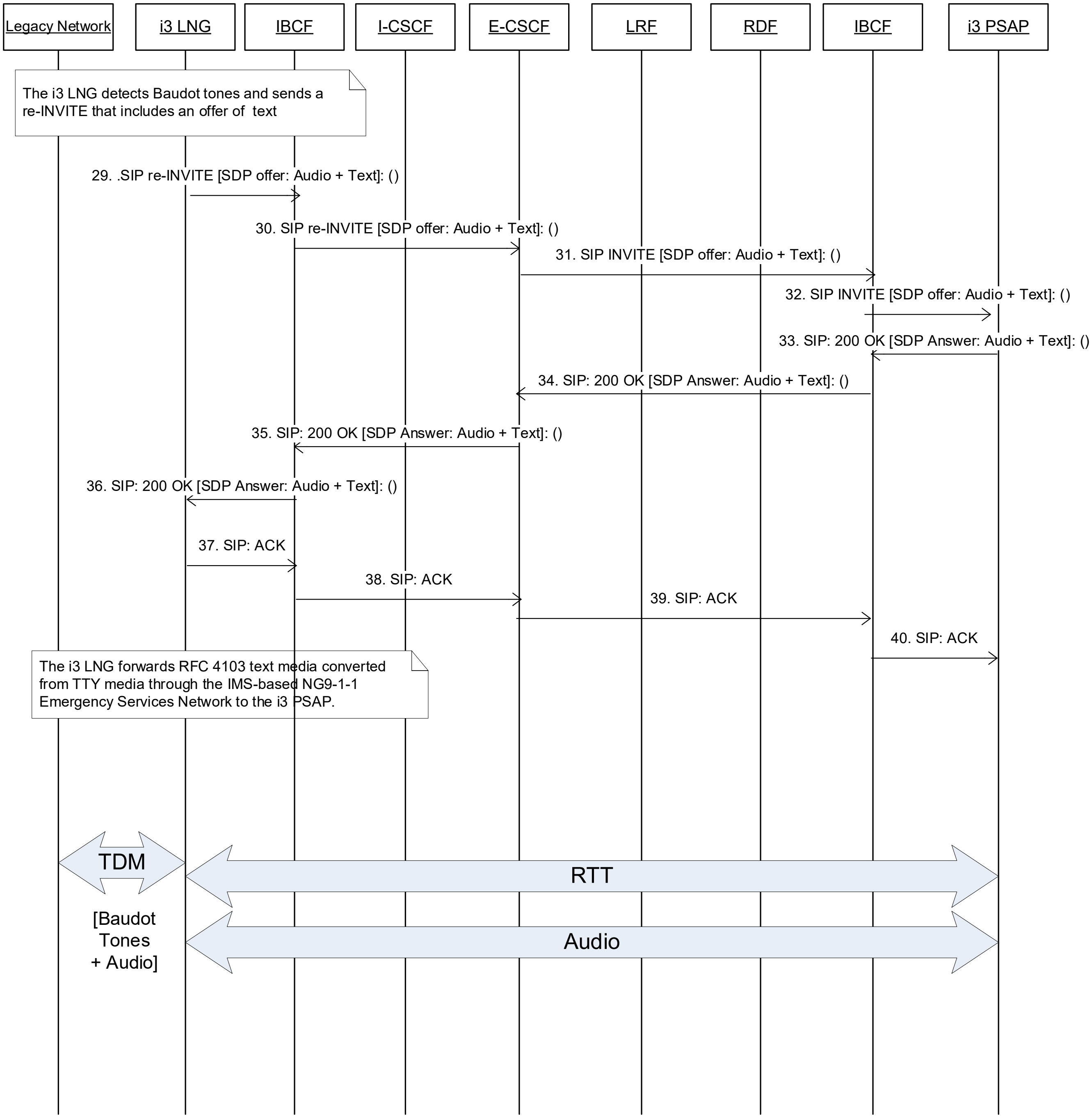

Legacy Network
i3 LNG
IBCF
I-CSCF
E-CSCF
LRF
RDF
IBCF
i3 PSAP
The i3 LNG detects Baudot tones and sends a re-INVITE that includes an offer of text
29. .SIP re-INVITE [SDP offer: Audio + Text]: ()
30. SIP re-INVITE [SDP offer: Audio + Text]: ()
31. SIP INVITE [SDP offer: Audio + Text]: ()
32. SIP INVITE [SDP offer: Audio + Text]: ()
33. SIP: 200 OK [SDP Answer: Audio + Text]: ()
34. SIP: 200 OK [SDP Answer: Audio + Text]: ()
35. SIP: 200 OK [SDP Answer: Audio + Text]: ()
36. SIP: 200 OK [SDP Answer: Audio + Text]: ()
37. SIP: ACK
38. SIP: ACK
39. SIP: ACK
40. SIP: ACK
The i3 LNG forwards RFC 4103 text media converted from TTY media through the IMS-based NG9-1-1 Emergency Services Network to the i3 PSAP.
TDM
[Baudot Tones + Audio]
RTT
Audio

**Figure 8.17: TTY Calls from Legacy Originating Network to an i3 PSAP via NG9-1-1 – Part II**

**Step 29.** Upon detecting the presence of Baudot tones, the i3 LNG generates a SIP re-INVITE message that includes an offer in the SDP describing a media format associated with real-time text (as specified in RFC 4103 [Ref 29]), and sends the SIP re-INVITE message to the IBCF. The re-INVITE message shall reference the existing dialog so that the i3 PSAP  knows that it is requesting modification of an existing session instead of establishing a new session.

**Step 30.** The IBCF forwards the SIP re-INVITE message to the E-CSCF.

**Step 31.** The E-CSCF forwards the SIP re-INVITE message to the (egress) IBCF.

**Step 32.** The IBCF forwards the SIP re-INVITE message to the i3 PSAP.

**Step 33.** The i3 PSAP returns a 200 OK message with [SDP Answer: Audio + Text] to the (egress) IBCF.

**Step 34.** The IBCF passes the 200 OK message to the E-CSCF.

**Step 35.** The E-CSCF passes the 200 OK message to the IBCF.

**Step 36.** The IBCF passes the 200 OK message to the i3 LNG.

**Step 37.** The i3 LNG returns an ACK to the IBCF in response to the 200 OK message.

**Step 38.** The IBCF passes the ACK to the E-CSCF.

**Step 39.** The E-CSCF passes the ACK to the (egress) IBCF.

**Step 40.** The IBCF passes the ACK to the i3 PSAP.

In this scenario, the incoming media from a legacy network will be Baudot tones. The i3 LNG, upon detecting the Baudot tones, converts the media to RFC 4103 [Ref 29] text format for transport over the NG9-1-1 network. The i3 LNG establishes a text media session in addition to the audio media session established by the initial SIP INVITE message. The i3 LNG sends the RFC 4103 [Ref 29] text media that has been converted from the Baudot tones forward to the i3 PSAP. Since the call is targeted towards an i3 PSAP, there is no further conversion needed and the media is forwarded as it is to the i3 PSAP.

### 8.7.3 TTY Calls from Legacy Originating Network to a Legacy PSAP via NG9-1-1

This call flow illustrates a TTY emergency call originating in a legacy circuit switched network terminated at a legacy PSAP that is served by an IMS-based NG9-1-1 Emergency Services Network, via an LPG. Similar to the scenario in Clause 8.7.2, since the call originated in a legacy network, the i3 LNG will initially setup the incoming emergency call with Audio media. This call flow example assumes that the incoming call is received by the NG9-1-1 Emergency Services Network with LbyV.

On the terminating side of the call flow, the LPG is responsible for translating incoming Text media to Baudot tones before forwarding the media to the legacy PSAP. The LPG is also responsible for recognizing Baudot tones in incoming media from the legacy PSAP and replacing them with RFC 4103 [Ref 29] text.

In this call flow example, an emergency call originating from a TTY user is presented to the PSAP as a “silent” call. Based on existing SOPs, the legacy PSAP attempts to establish communication with the caller by generating Baudot tones toward the caller.  Upon detecting the Baudot tones from the legacy PSAP, the LPG generates a re-INVITE message to request the establishment of a real-time text media session over which the RFC 4013 real-time text (converted from the incoming Baudot tones) can be sent. The LPG must buffer any real-time text that is converted from the received Baudot tones until such time as the text media session is established (i.e., until a 200 OK message is received from the LNG/NG9-1-1 Emergency Services Network in response to the re-INVITE) and the real-time text can be passed toward the caller. See Clause 6.2 of NENA-STA-010.3 [Ref 27] for further details regarding RTT-TTY interworking at an i3 LPG.

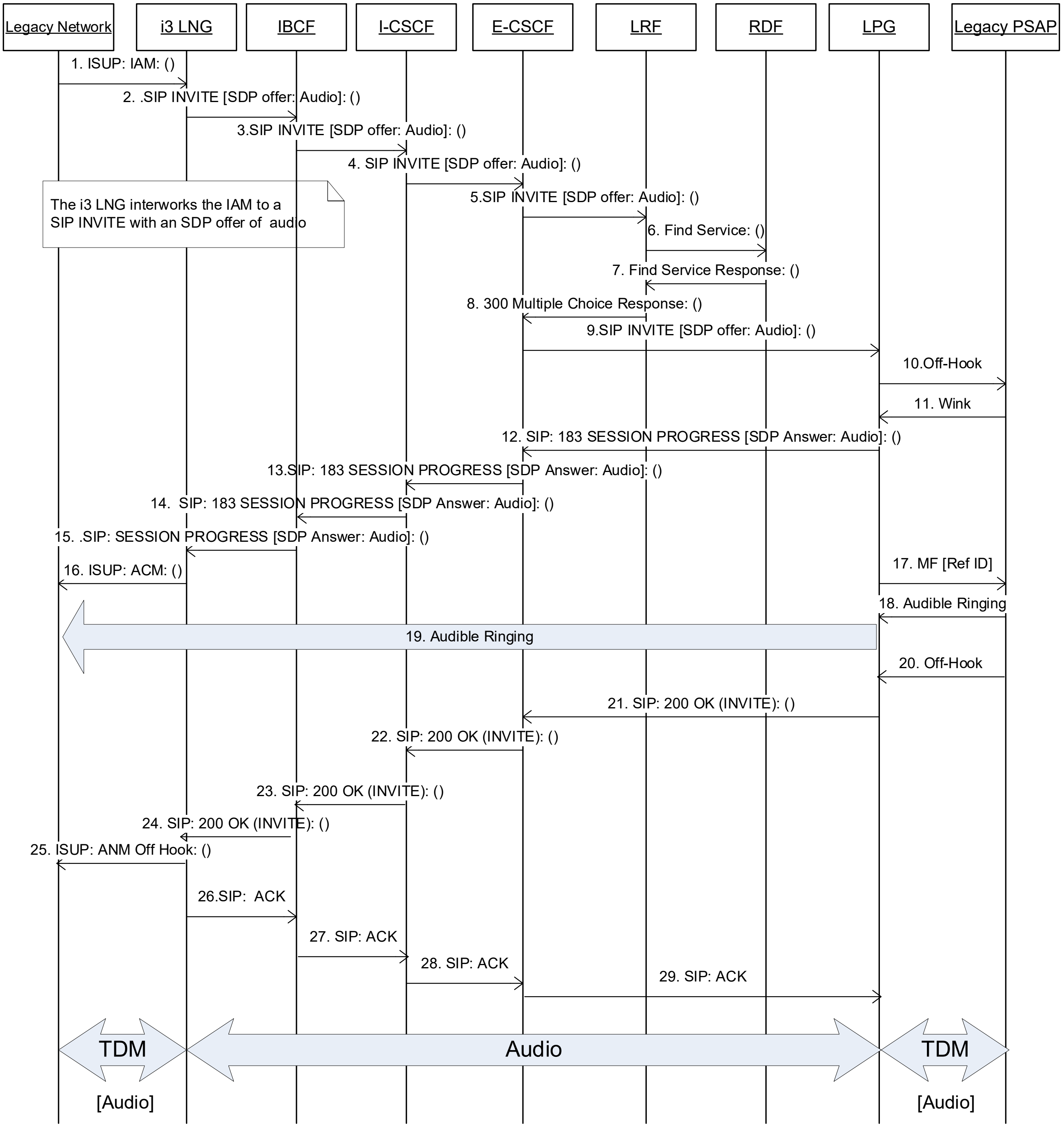

Legacy Network
i3 LNG
IBCF
I-CSCF
E-CSCF
LRF
RDF
LPG
Legacy PSAP
1. ISUP: IAM: ()
2. .SIP INVITE [SDP offer: Audio]: ()
3.SIP INVITE [SDP offer: Audio]: ()
4. SIP INVITE [SDP offer: Audio]: ()
The i3 LNG interworks the IAM to a SIP INVITE with an SDP offer of audio
5.SIP INVITE [SDP offer: Audio]: ()
6. Find Service: ()
7. Find Service Response: ()
8. 300 Multiple Choice Response: ()
9.SIP INVITE [SDP offer: Audio]: ()
10.Off-Hook
11. Wink
12. SIP: 183 SESSION PROGRESS [SDP Answer: Audio]: ()
13.SIP: 183 SESSION PROGRESS [SDP Answer: Audio]: ()
14. SIP: 183 SESSION PROGRESS [SDP Answer: Audio]: ()
15. .SIP: SESSION PROGRESS [SDP Answer: Audio]: ()
16. ISUP: ACM: ()
17. MF [Ref ID]
18. Audible Ringing
19. Audible Ringing
20. Off-Hook
21. SIP: 200 OK (INVITE): ()
22. SIP: 200 OK (INVITE): ()
23. SIP: 200 OK (INVITE): ()
24. SIP: 200 OK (INVITE): ()
25. ISUP: ANM Off Hook: ()
26.SIP: ACK
27. SIP: ACK
28. SIP: ACK
29. SIP: ACK
TDM
[Audio]
Audio
TDM
[Audio]

**Figure 8.18: TTY Calls from Legacy Originating Network to a Legacy PSAP via NG9-1-1 – Part I**

**Step 1.** The ingress i3 LNG receives an SS7 IAM message from the legacy network.

**Step 2.** The i3 LNG detects an emergency call originating from a legacy network, interworks the incoming signaling to SIP with a request to setup Audio media, and a media feature tag of “urn:nena:media-feature.TTY-interworking”, and forwards the SIP INVITE to the IBCF.

**Step 3.** The IBCF forwards the SIP INVITE to the I-CSCF.

**Step 4.** The I-CSCF forwards the SIP INVITE to the pre-configured E-CSCF.

**Step 5.** The E-CSCF forwards the SIP INVITE to the LRF.

**Step 6.** The LRF queries the RDF using the location information received in the body of the received SIP INVITE message.

**Step 7.** The RDF returns a Route URI. In this example, the Route URI is associated with a legacy PSAP that is served by the IMS-based NG9-1-1 Emergency Services Network.

**Step 8.** The LRF redirects the call back to the E-CSCF, passing the Route (PSAP) URI in a 300 Multiple Choices response.

**Step 9.** The E-CSCF generates an outgoing SIP INVITE message, using the information received from the LRF as well as information received in the initial SIP INVITE message, and forwards it to the LPG. The SIP INVITE message contains the PSAP URI in the Route header.

**Step 10.** The LPG generates an off-hook signal toward the legacy PSAP.

**Step 11.** The legacy PSAP returns a wink signal back to the LPG.

**Step 12.** The LPG sends a SIP: 183 SESSION PROGRESS (with an SDP Answer and a media feature tag of “urn:nena:media-feature.TTY-interworking”) to the E-CSCF.

**Step 13.** The E-CSCF forwards the SIP: 183 SESSION PROGRESS message to I-CSCF.

**Step 14.** The I-CSCF forwards the SIP: 183 SESSION PROGRESS to the IBCF.

**Step 15.** The IBCF forwards the SIP: 183 SESSION PROGRESS to the i3 LNG.

**Step 16.** The i3 LNG interworks the SIP: 183 SESSION PROGRESS message to an SS7 ACM towards the legacy network.

**Step 17.** The LPG delivers the call to the legacy PSAP, mapping the SIP signaling from the incoming INVITE message to the outgoing Traditional or Enhanced MF signaling sequences. (Note that this can happen any time after step 11, in parallel with the 183 SESSION PROGRESS message being passed toward the i3 LNG.)

**Step 18.** The legacy PSAP sends Audible Ringing back to LPG.

**Step 19.** The Audible Ringing is delivered to the legacy network as Early Media: Audible Ringing Delivered.

**Step 20.** When the PSAP answers the call, it returns an off-hook signal back to the LPG.

**Step 21.** The LPG maps the off-hook signal to a SIP: 200 OK message and forwards the SIP: 200 OK message to the E-CSCF.

**Step 22.** The E-CSCF passes the SIP: 200 OK message to the I-CSCF.

**Step 23.** The I-CSCF passes the SIP: 200 OK message to the IBCF.

**Step 24.** The IBCF passes the SIP: 200 OK message to the i3 LNG.

**Step 25.** The i3 LNG maps the SIP: 200 OK message to an SS7 ANM message towards the legacy network.

**Step 26.** The i3 LNG returns a SIP: ACK message toward the IBCF.

**Step 27.** The IBCF sends a SIP: ACK to the I-CSCF.

**Step 28.** The I-CSCF sends a SIP: ACK to the E-CSCF.

**Step 29.** The E-CSCF sends a SIP: ACK to the LPG.

At this point in the call flow, audio media is allowed to flow, but the legacy PSAP only hears silence. As a result, following SOPs for “silent” calls, the legacy PSAP generates Baudot tones toward the caller.

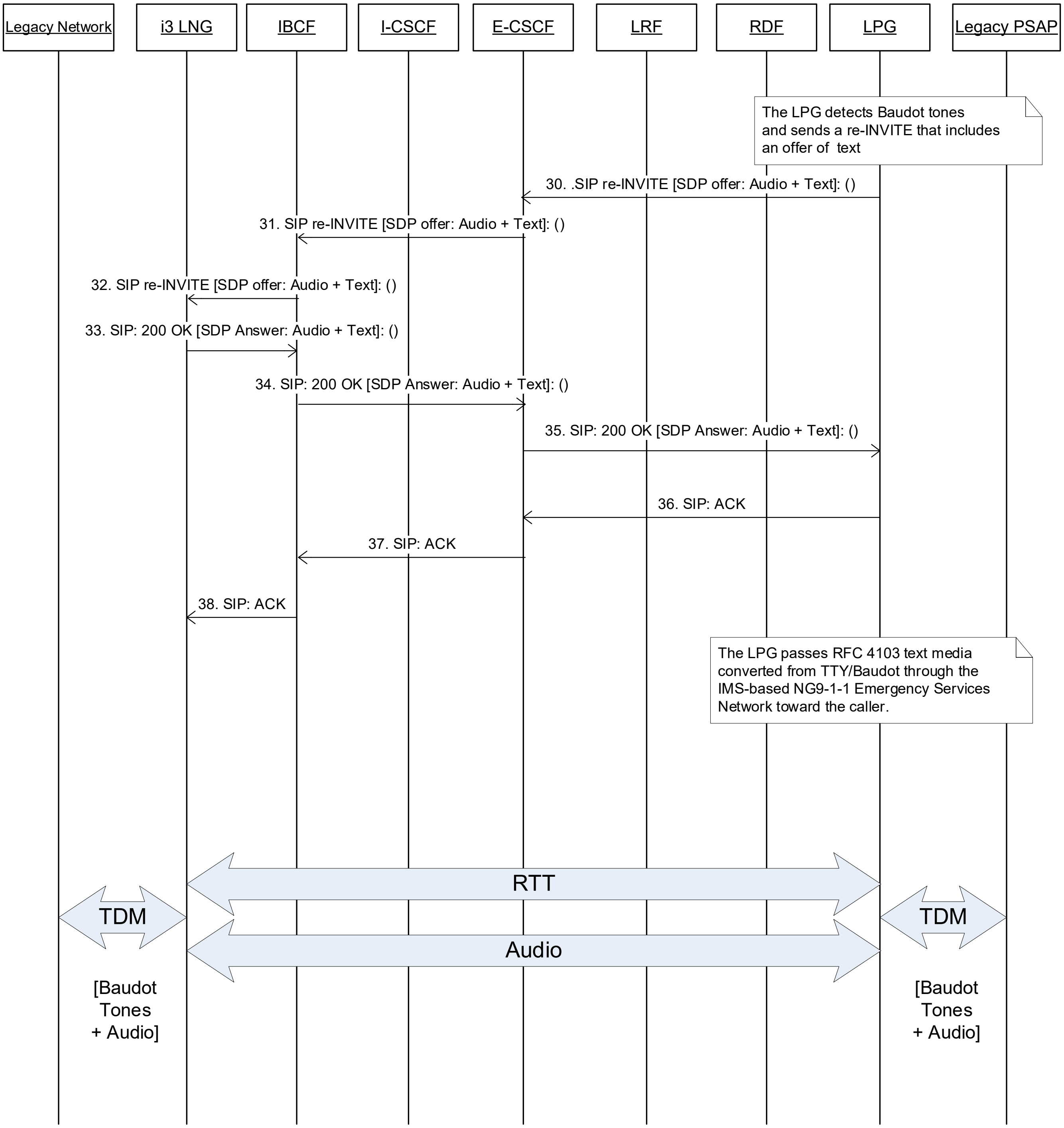

Legacy Network
i3 LNG
IBCF
I-CSCF
E-CSCF
LRF
RDF
LPG
Legacy PSAP
The LPG detects Baudot tones and sends a re-INVITE that includes an offer of  text
30. .SIP re-INVITE [SDP offer: Audio + Text]: ()
31. SIP re-INVITE [SDP offer: Audio + Text]: ()
32. SIP re-INVITE [SDP offer: Audio + Text]: ()
33. SIP: 200 OK [SDP Answer: Audio + Text]: ()
34. SIP: 200 OK [SDP Answer: Audio + Text]: ()
35. SIP: 200 OK [SDP Answer: Audio + Text]: ()
36. SIP: ACK
37. SIP: ACK
38. SIP: ACK
The LPG passes RFC 4103 text media converted from TTY/Baudot through the IMS-based NG9-1-1 Emergency Services Network toward the caller.
RTT
TDM
Audio
TDM
[Baudot Tones + Audio]
[Baudot Tones + Audio]

**Figure 8.19: TTY Calls from Legacy Originating Network to a Legacy PSAP via NG9-1-1 – Part II**

**Step 30.** Upon detecting the presence of Baudot tones, the LPG generates a SIP re-INVITE message that includes an offer in the SDP describing a media format associated with real-time text (as specified in RFC 4103 [Ref 29]), and sends the SIP re-INVITE message to the E-CSCF. The re-INVITE message references the existing dialog so that the i3 LNG knows that it is requesting modification of an existing session instead of establishing a new session.

**Step 31.** The E-CSCF forwards the SIP re-INVITE message to the IBCF.

**Step 32.** The IBCF forwards the SIP re-INVITE message to the i3 LNG.

**Step 33.** The i3 LNG returns a 200 OK message with [SDP Answer: Audio + Text] to the IBCF.

**Step 34.** The IBCF passes the 200 OK message to the E-CSCF.

**Step 35.** The E-CSCF passes the 200 OK message to the LPG.

**Step 36.** The LPG returns an ACK to the E-CSCF in response to the 200 OK message.

**Step 37.** The E-CSCF passes the ACK to the IBCF.

**Step 38.** The IBCF passes the ACK to the i3 LNG.

The i3 LNG interworks the RFC 4103 [Ref 29] text media to Baudot tones for delivery to the TTY caller. If the i3 LNG receives (i.e., from a legacy PSAP/LPG) simultaneous RFC 4103 [Ref 29] real-time text and audio media that may include Baudot tones or other sounds, the i3 LNG must notch the audio frequencies used for Baudot tones from the received audio media and then insert the Baudot tones transcoded from the received RFC 4103 [Ref 29] text to minimize the distortion of the Baudot tones delivered to the caller. See Clause 6.1 of NENA-STA-010.3 [Ref 27] for further details regarding RTT-TTY interworking at an i3 LNG.

## *8.8 Call Transfer/Bridging*

A fundamental capability of E9-1-1/NG9-1-1 is the ability to transfer emergency calls. IMS-based NG9-1-1 Emergency Services Networks must support the attended transfer, as well as the blind transfer of emergency calls between PSAPs that are served by the IMS-based NG9-1-1 Emergency Services Network. This includes transfers initiated by i3 PSAPs toward legacy PSAPs and other i3 PSAPs, as well as transfers initiated by legacy PSAPs toward i3 PSAPs and other legacy PSAPs.

The conferencing/transfer procedures to support attended transfers are based on 3GPP TS 24.147 [Ref 11], RFC 4353 [Ref 13], NENA-STA-010.3 [Ref 27], RFC 4579 [Ref 22], and RFC 3891 [Ref 35]. The blind transfer procedures are based on 3GPP TS 24.629 [Ref 49], NENA-STA-010.3 [Ref 27], and RFC 3515 [Ref 50].

The conference/transfer functions associated with attended transfers are provided by replacing the existing signaling/media path between the caller and the transfer-from PSAP with a new signaling/media path that involves the conferencing resources (e.g., MRFC/MRFP). In the context of blind transfers, the existing signaling/media path between the caller and the transfer-from PSAP are replaced by a new signaling/media path between the caller and the transfer-to PSAP. This standard provides two methods of media anchoring:

- Conditionally at the Ingress point of the IMS emergency services network.
- At the Egress point of the IMS emergency services network.

The point that provides the signaling media anchoring within the IMS emergency services network shall be able to support the “Replaces” header field present in an incoming INVITE request and act upon it according to RFC 3891 [Ref 35]. It shall also include the “Replaces” option tag in the Supported header field in the initial dialogue request.

Clause 8.8.1 covers the attended transfer scenarios where the transfer-from PSAP is an i3 PSAP:

- Clause 8.8.1.1 provides call flows that allow B2BUA functionality with header replacement and media anchoring at the originating network-facing IBCF when the signaling/media anchoring is done at the Ingress point for transfers initiated by a transfer-from i3 PSAP.
- Clause 8.8.1.2 provides call flows that allow B2BUA functionality with header replacement and media anchoring at the transfer-from PSAP-facing IBCF when the signaling/media anchoring is done at the egress point for transfers initiated by a transfer-from i3 PSAP.

Clause 8.8.2 covers the attended transfer scenarios where the transfer-from PSAP is a legacy PSAP:

- Clause 8.8.2.1 provides call flows that allow B2BUA functionality with header replacement and media anchoring at the transfer-from PSAP-facing IBCF when the signaling/media anchoring is done at the ingress point for transfers initiated by a transfer-from legacy PSAP.
- Clause 8.8.2.2 provides call flows that allow B2BUA functionality with header replacement and media anchoring at the transfer-from PSAP-facing IBCF when the signaling/media anchoring is done at the egress point for transfers initiated by a transfer-from legacy PSAP.

Clause 8.8.3 covers the blind transfer scenarios where the transfer-from PSAP is an i3 PSAP:

- Clause 8.8.3.1 provides call flows that allow B2BUA functionality with header replacement and media anchoring at the transfer-from PSAP-facing IBCF when the signaling/media anchoring is done at the ingress point for transfers initiated by a transfer-from i3 PSAP.
- Clause 8.8.3.2 provides call flows that allow B2BUA functionality with header replacement and media anchoring at the transfer-from PSAP-facing IBCF when the signaling/media anchoring is done at the egress point for transfers initiated by a transfer-from i3 PSAP.

### 8.8.1 Support for Attended Emergency Call Transfer Requests from i3 PSAPs to Transfer-to PSAPs/Destinations

When an i3 PSAP initiates an attended transfer, it must first create a conference on a bridge. In the context of an IMS-based NG9-1-1 Emergency Services Network, this bridge will support multimedia (voice, video, text) and will reside in a conferencing Application Server (AS), as described in 3GPP TS 24.147 [Ref 11]. Bridging is necessary to support the attended transfer of emergency calls which require that a new party (e.g., a call taker at a transfer-to PSAP) be added to the call before the transfer-from PSAP (i.e., the original call taker at the PSAP that initially answered the call) disconnects from the call, without the caller ever being put on hold.

For SIP-based conferences, the conferencing AS implements the role of a conference focus, as described in Clause 5.3.2 of 3GPP TS 24.147 [Ref 11]. Media control for the conference is provided by a Media Resource Function Controller (MRFC) and media mixing is provided by a Media Resource Function Processor (MRFP) in the IMS-based NG9-1-1 Emergency Services Network. Consistent with Clause 4 of 3GPP TS 24.147 [Ref 11], these functional elements will be configured as depicted in Figure 8-18 below.

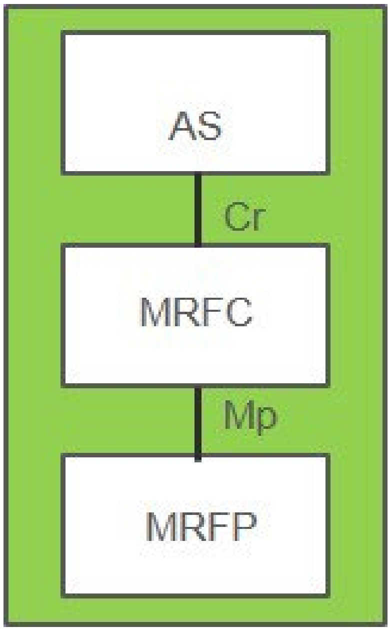


**Figure 8.20: Conferencing Functional Architecture**

3GPP TS 24.147 [Ref 11] also describes the use of an Event package that allows conference participants to manage a conference by subscribing to the conference event package, as described in RFC 4575 [Ref 31].

The following subclauses describe the flows associated with a transfer that is initiated by an i3 PSAP.

### 8.8.1.1 Signaling/Media Anchoring at Ingress Point Conditional on Supported Header

While the procedures described in RFC 4579 [Ref 22] for establishing a SIP conference assume that the calling device supports the Replaces header, this standard does not assume or require support of the Replaces header by the calling device. In those cases where the Replaces header is not supported by the calling device, this clause describes transfer procedures in which the INVITE method with the Replaces header generated by the conferencing AS will be directed to an originating network-facing IBCF operating as a B2BUA rather than to the calling device. Specifically, if an originating network-facing IBCF in an IMS-based NG9-1-1 Emergency Services Network receives a SIP INVITE that does not include a Supported header containing the Replaces option-tag (which will be the case for emergency calls delivered by IMS originating networks that follow the procedures specified in ATIS-0700015), the originating network-facing IBCF will act as a B2BUA (as described in Clause 5.10 of 3GPP TS 24.229 [Ref 2]) and will include a Supported header containing the Replaces option-tag in the INVITE forwarded to the I-CSCF.

#### 8.8.1.1.1 Conference Establishment

The flow depicted in Figure 8-19 illustrates the mechanism by which an i3 PSAP creates a conference at a conferencing AS. This call flow assumes that upon receiving an emergency session request (i.e., a session request in which the Request-URI contains a service URN in the “sos” tree [e.g., “urn:service:sos”]), the originating network-facing IBCF will determine whether or not the incoming SIP INVITE message includes a Supported header containing the Replaces option-tag. If it does not, the IBCF will act as a B2BUA and include a Supported header containing the Replaces option-tag in the outgoing SIP INVITE message that it sends to the I-CSCF. Normal call processing will be applied to the emergency call as it progresses through the IMS-based NG9-1-1 Emergency Services Network and is delivered to the i3 PSAP via a PSAP-facing IBCF (not shown) that is operating as a proxy (or as a B2BUA that does not modify received headers, as described in RFC 7092 [Ref 33]). In this example, the (transfer-from) i3 PSAP determines that the call must be transferred and creates a conference to support the transfer of the emergency call. This call flow assumes that the calling device does not support the Replaces header. In addition, this call flow assumes that all signaling to/from the conferencing AS/MRFC to establish the initial conference between the transfer-from PSAP and the conferencing AS/MRFC flows through the I-CSCF.

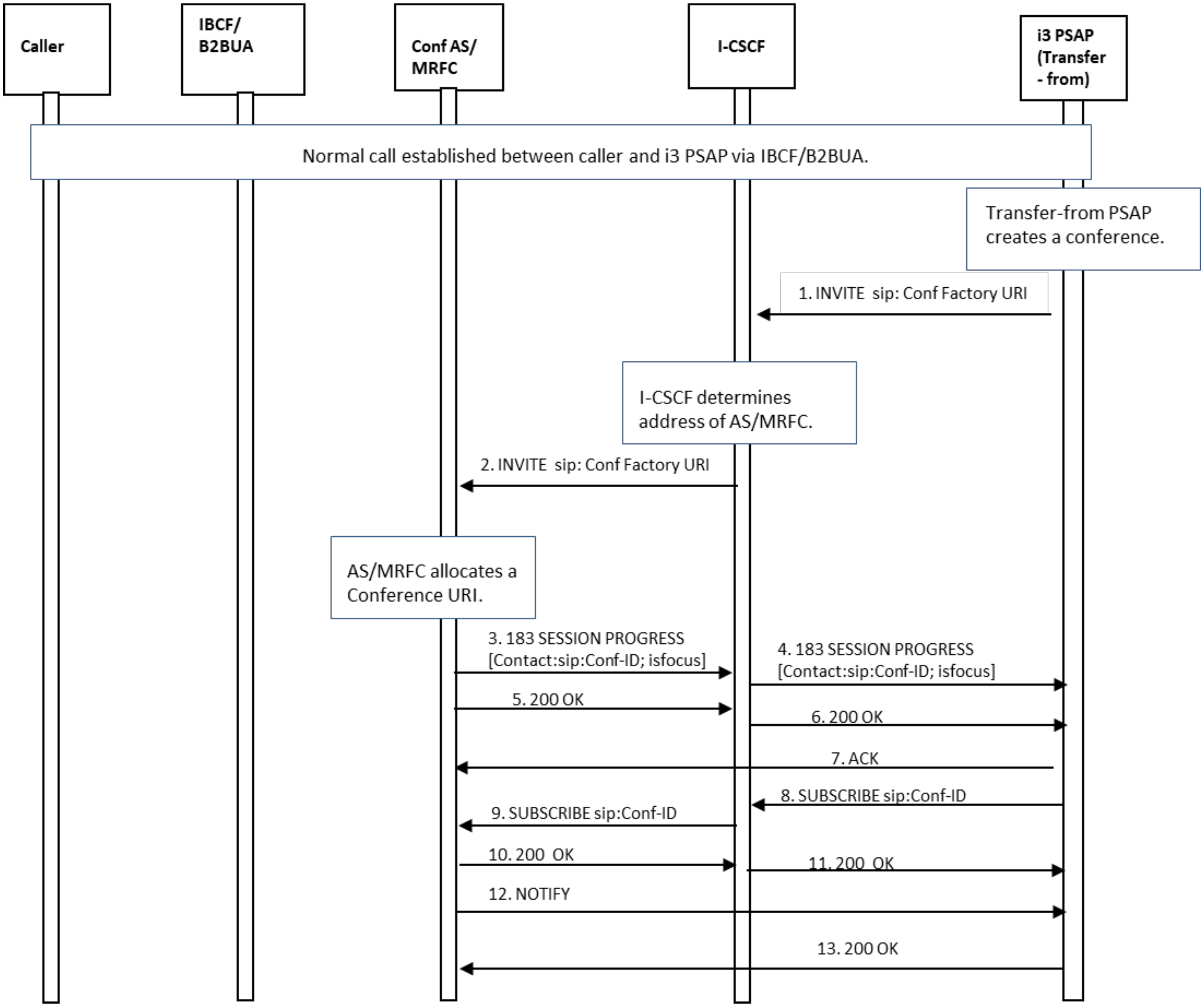

Caller
IBCF/ B2BUA
Conf AS/ MRFC
I-CSCF
i3 PSAP (Transfer - from)
Normal call established between caller and i3 PSAP via IBCF/B2BUA.
Transfer-from PSAP creates a conference.
1. INVITE sip: Conf Factory URI
I-CSCF determines address of AS/MRFC.
2. INVITE sip: Conf Factory URI
AS/MRFC allocates a Conference URI.
3. 183 SESSION PROGRESS [Contact:sip:Conf-ID; isfocus]
4. 183 SESSION PROGRESS [Contact:sip:Conf-ID; isfocus]
5. 200 OK
6. 200 OK
7. ACK
8. SUBSCRIBE sip:Conf-ID
9. SUBSCRIBE sip:Conf-ID
10. 200 OK
11. 200 OK
12. NOTIFY
13. 200 OK

**Figure 8.21: i3 PSAP Establishes Conference with Conferencing AS/MRFC**

**Step 1.** The transfer-from PSAP determines that it needs to transfer an emergency call and therefore must create a conference using an AS/MRFC in the IMS-based NG9-1-1 Emergency Services Network. The transfer-from i3 PSAP creates the conference by first sending an INVITE (via an IBCF [not shown]) to an I-CSCF in the IMS-based NG9-1-1 Emergency Services Network, using a conference factory URI that is known by/provisioned at the transfer-from i3 PSAP. The SIP INVITE message will include a Resource Priority Header set to "esnet.1" to indicate that the session request is associated with the transfer of an emergency call.

*The I-CSCF resolves the conference factory URI and determines the address of the conferencing AS/MRFC.*

**Step 2.** The I-CSCF forwards the SIP INVITE message to the conferencing AS/MRFC. The I-CSCF does not add itself to the Record-Route header since it does not need to remain in the signaling path for subsequent requests.

*The conferencing AS/MRFC allocates a conference URI, based on local information, information gained from the conference-factory URI, and other information received in SIP signaling.*

**Step 3.** The conferencing AS/MRFC responds to the INVITE by returning a 183 SESSION PROGRESS message to the I-CSCF. The Contact header contains the conference URI for the conference allocated at the AS/MRFC and the isfocus feature parameter.

**Step 4.** The I-CSCF passes the 183 SESSION PROGRESS message (via an IBCF [not shown]) to the transfer-from i3 PSAP.

**Step 5.** The conferencing AS/MRFC then returns a 200 OK message to the I-CSCF, to establish a session with the transfer-from i3 PSAP.

**Step 6.** The I-CSCF sends a 200 OK message (via an IBCF [not shown]) to the transfer-from i3 PSAP.

**Step 7.** The transfer-from i3 PSAP returns an ACK message to the conferencing AS/MRFC (via an IBCF [not shown]) in response to the 200 OK message.

*A session is established between the transfer-from i3 PSAP and the conferencing AS/MRFC. Note that the media session between the IBCF/B2BUA and the transfer-from i3 PSAP still exists at this time.*

**Step 8.** The transfer-from i3 PSAP subscribes to the conference associated with the URI obtained from the Contact header provided by the conferencing AS/MRFC in the 180 SESSION PROGRESS message by sending a SIP SUBSCRIBE message containing the Conference ID via an IBCF (not shown) to the I-CSCF.

**Step 9.** The I-CSCF sends the SIP SUBSCRIBE message to the conferencing AS/MRFC. The I-CSCF does not add itself to the Record-Route header since it does not need to remain in the signaling path for subsequent requests.

**Step 10.** The conferencing AS/MRFC acknowledges the subscription request by sending a 200 OK message to the I-CSCF.

**Step 11.** The I-CSCF passes the 200 OK message back to the transfer-from i3 PSAP via an IBCF (not shown).

**Step 12.** The conferencing AS/MRFC then returns a NOTIFY message to the transfer-from i3 PSAP via an IBCF (not shown) to provide subscription status information.

**Step 13.** The i3 PSAP responds by returning a 200 OK message via an IBCF (not shown) to the AS/MRFC.

#### 8.8.1.1.2 Transfer-from PSAP Requests that the Conferencing AS Invite the IBCF/B2BUA to the Conference

Having established the conference, the transfer-from i3 PSAP asks the conferencing AS/MRFC to invite the IBCF/B2BUA to the conference. As specified above, this flow assumes that the calling device does not support the Replaces header and that the PSAP-facing IBCF (not shown) is operating as a proxy.

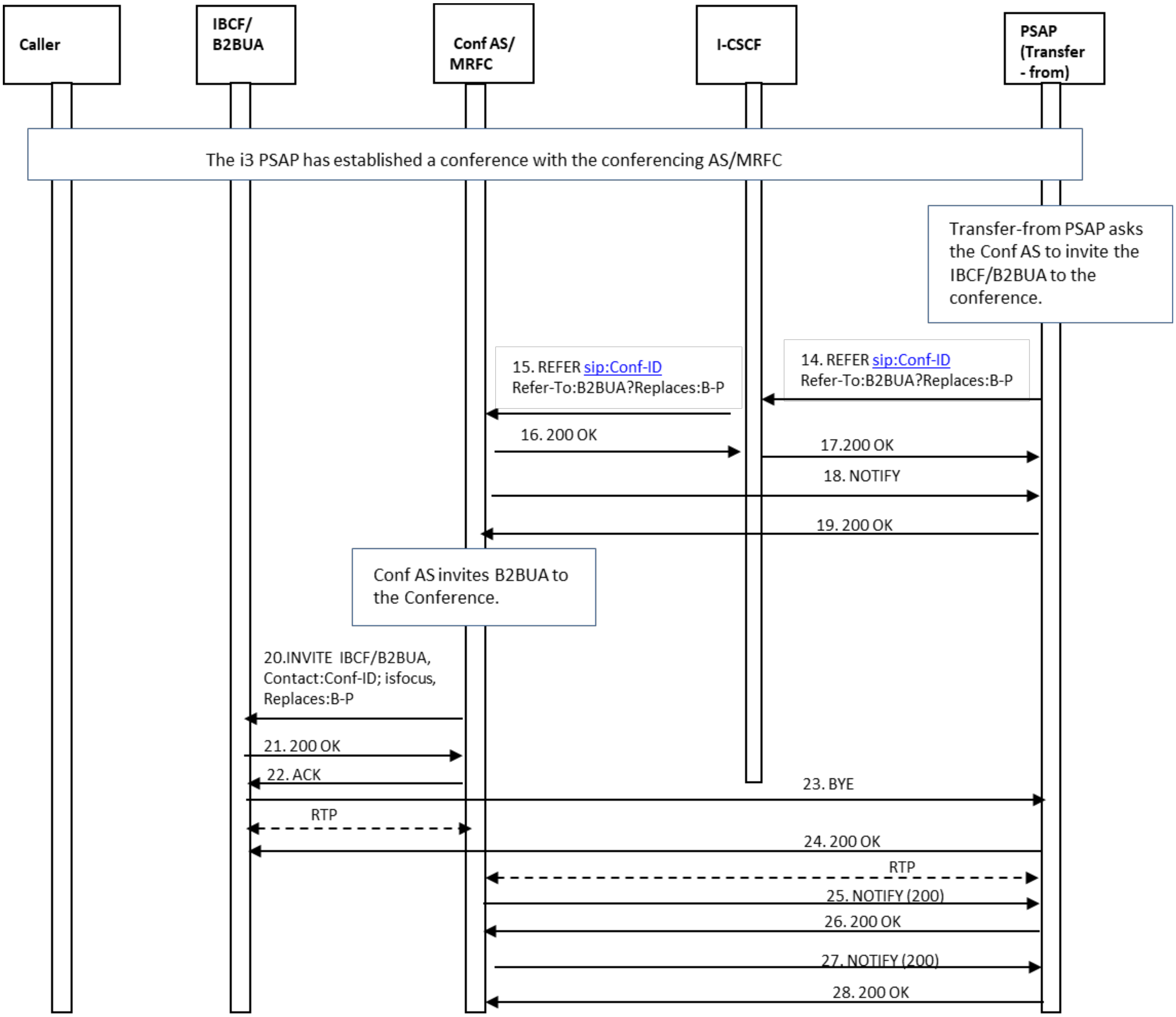

Caller
IBCF/ B2BUA
Conf AS/ MRFC
I-CSCF
PSAP (Transfer - from)
The i3 PSAP has established a conference with the conferencing AS/MRFC
Transfer-from PSAP asks the Conf AS to invite the IBCF/B2BUA to the conference.
14. REFER sip:Conf-ID Refer-To:B2BUA?Replaces:B-P
15. REFER sip:Conf-ID Refer-To:B2BUA?Replaces:B-P
16. 200 OK
17.200 OK
18. NOTIFY
19. 200 OK
Conf AS invites B2BUA to the Conference.
20.INVITE IBCF/B2BUA, Contact:Conf-ID; isfocus, Replaces:B-P
21. 200 OK
22. ACK
23. BYE
RTP
24. 200 OK
RTP
25. NOTIFY (200)
26. 200 OK
27. NOTIFY (200)
28. 200 OK

**Figure 8.22: i3 PSAP Requests that IBCF/B2BUA be Invited to the Conference**

**Step 14.** The transfer-from i3 PSAP sends a REFER method to the I-CSCF (via an IBCF [not shown]).

**Step 15.** The I-CSCF passes the REFER method to the conferencing AS/MRFC. The I-CSCF does not add itself to the Record-Route header since it does not need to remain in the signaling path for subsequent requests. The REFER method requests that the conferencing AS/MRFC invite the IBCF/B2BUA to the conference. The REFER method contains an escaped Replaces header field in the URI included in the Refer-To header field.

**Step 16.** The conferencing AS/MRFC returns a 200 OK message to the I-CSCF.

**Step 17.** The I-CSCF passes the 200 OK message (via an IBCF [not shown]) to the transfer-from i3 PSAP.

**Step 18.** The conferencing AS/MRFC then returns a NOTIFY message (via an IBCF [not shown]) to the transfer-from i3 PSAP, indicating the subscription state of the REFER request (i.e., active).

**Step 19.** The transfer-from i3 PSAP returns a 200 OK message (via an IBCF [not shown]) in response to the NOTIFY message.

**Step 20.** The conferencing AS/MRFC invites the IBCF/B2BUA to the conference by sending it an INVITE method containing the Conf-ID and a Replaces header that references the leg between the IBCF/B2BUA and the transfer-from PSAP.

**Step 21.** The IBCF/B2BUA accepts the invitation by returning a 200 OK message to the conferencing AS/MRFC.

**Step 22.** The conferencing AS/MRFC acknowledges receipt of the 200 OK message by returning an ACK.

*A session is established between the IBCF/B2BUA and the conferencing AS/MRFC. Note that the media session between the IBCF/B2BUA and the transfer-from i3 PSAP still exists at this time. Note also that the media session between the caller and the IBCF/B2BUA is undisturbed.*

**Step 23.** The IBCF/B2BUA terminates the session with the transfer-from i3 PSAP by sending a BYE message (via an IBCF [not shown], following the signaling path established by the INVITE request associated with the original emergency session) to the transfer-from i3 PSAP.

*At this point, the IBCF/B2BUA switches the media from the session with the transfer-from i3 PSAP to the session with the conferencing AS/MRFC.*

**Step 24.** The transfer-from i3 PSAP responds by returning a 200 OK message (via an IBCF [not shown]).

*At this point, the transfer-from i3 PSAP switches the media to the session with the conferencing AS/MRFC and the session between the IBCF/B2BUA and the transfer-from PSAP is terminated.*

**Step 25.** The conferencing AS/MRFC sends a NOTIFY message to the transfer-from i3 PSAP (via an IBCF [not shown]) to provide updated status of the subscription associated with the REFER request.

**Step 26.** The transfer-from i3 PSAP responds by returning a 200 OK message (via an IBCF [not shown]).

**Step 27.** The conferencing AS/MRFC sends a NOTIFY message to the transfer-from i3 PSAP (via an IBCF [not shown]) to provide updated status of the subscription associated with the REFER request.

**Step 28.** The transfer-from i3 PSAP responds by returning a 200 OK message to the conferencing AS/MRFC (via an IBCF [not shown]).

#### 8.8.1.1.3 Transfer-from PSAP Requests that the Conferencing AS Invite the Transfer-to PSAP to the Conference

Having invited the IBCF/B2BUA to the conference, the i3 PSAP then requests that the conferencing AS/MRFC invite the transfer-to PSAP to the conference, using the mechanisms defined in RFC 4579 [Ref 22], as illustrated in Figure 8-21 and Figure 8-22. The i3 PSAP will query an ECRF (not shown), using a service URN in the “urn:emergency:service:responder” family and the location information received with the call, to support “selective transfer” of emergency calls. The i3 PSAP will then use the URI returned in the response from the ECRF to populate the Refer-To header of the outgoing REFER method. When a transfer-from i3 PSAP handles a call, it develops information about the call that must be passed to subsequent PSAPs, dispatchers, and/or responders. This information is included in an Additional Data structure referred to as an Emergency Incident Data Object (EIDO). When, in the process of transferring an emergency call, an i3 PSAP requests that the conferencing AS invite the transfer-to PSAP to the conference, the transfer-from i3 PSAP will include a reference to an EIDO in the request it sends to the conferencing AS. The AS includes this reference in the Call-Info header of the SIP INVITE that it sends to the transfer-to PSAP/LPG. The transfer-to PSAP/LPG uses the EIDO reference URI to query the transfer-from PSAP for the EIDO.

### 8.8.1.1.3.1 Transfer-to PSAP is an i3 PSAP

Figure 8-21 illustrates a scenario where the transfer-to PSAP is an i3 PSAP. (Note that all SIP messages between the transfer-to i3 PSAP and the conferencing AS/MRFC flow via an IBCF [not shown].)

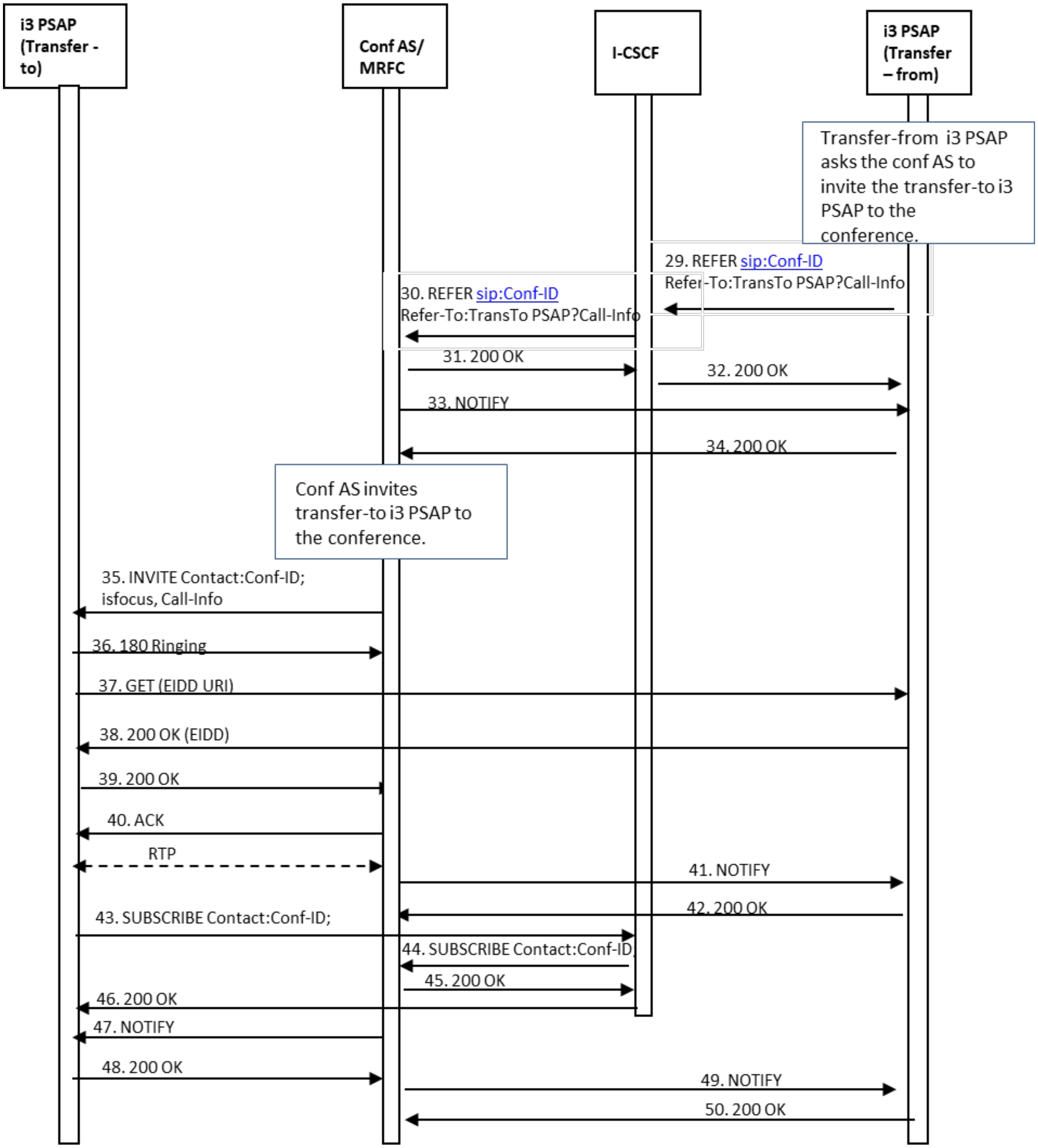

i3 PSAP (Transfer - to)
Conf AS/ MRFC
I-CSCF
i3 PSAP (Transfer – from)
Transfer-from i3 PSAP asks the conf AS to invite the transfer-to i3 PSAP to the conference.
29. REFER sip:Conf-ID Refer-To:TransTo PSAP?Call-Info
30. REFER sip:Conf-ID Refer-To:TransTo PSAP?Call-Info
31. 200 OK
32. 200 OK
33. NOTIFY
34. 200 OK
Conf AS invites transfer-to i3 PSAP to the conference.
35. INVITE Contact:Conf-ID; isfocus, Call-Info
36. 180 Ringing
37. GET (EIDD URI)
38. 200 OK (EIDD)
39. 200 OK
40. ACK
RTP
41. NOTIFY
42. 200 OK
43. SUBSCRIBE Contact:Conf-ID;
44. SUBSCRIBE Contact:Conf-ID;
45. 200 OK
46. 200 OK
47. NOTIFY
48. 200 OK
49. NOTIFY
50. 200 OK

**Figure 8.23: i3 PSAP Requests that a Transfer-to i3 PSAP be Invited to the Conference**

**Step 29.** The transfer-from i3 PSAP sends a REFER method to the I-CSCF (via an IBCF [not shown]).

**Step 30.** The I-CSCF passes the REFER method to the conferencing AS/MRFC. The I-CSCF does not add itself to the Record-Route header since it does not need to remain in the signaling path for subsequent requests. The REFER method requests that the conferencing AS/MRFC invite the transfer-to i3 PSAP to the conference. The REFER method contains the Conf-ID and a Refer-To header that contains the URI of the transfer-to i3 PSAP. The REFER method also contains an escaped Call-Info header field containing a reference URI that points to the EIDO data structure and a purpose parameter of "eido".

**Step 31.** The conferencing AS/MRFC returns a 200 OK message to the I-CSCF.

**Step 32.** The I-CSCF passes the 200 OK message (via an IBCF [not shown]) to the transfer-from i3 PSAP.

**Step 33.** The conferencing AS/MRFC then returns a NOTIFY message (via an IBCF [not shown]), indicating that subscription state of the REFER request (i.e., active).

**Step 34.** The transfer-from i3 PSAP returns a 200 OK message (via an IBCF [not shown]) in response to the NOTIFY message.

**Step 35.** The conferencing AS/MRFC invites the transfer-to i3 PSAP to the conference by sending an INVITE method (via a Transit Function/IBCF [not shown]) containing the Conf-ID and Contact header that contains the conference URI and the isfocus feature parameter. The INVITE also contains the Call-Info header field containing a reference URI that points to the EIDO data structure and a purpose parameter of "eido". The SIP INVITE message will include a Resource Priority Header set to "esnet.1" to indicate that the session request is associated with the transfer of an emergency call.

**Step 36.** The transfer-to i3 PSAP UA responds by returning a 180 RINGING message (via the IBCF/Transit Function [not shown]) to the conferencing AS/MRFC.

**Step 37.** The transfer-to i3 PSAP queries the transfer-from i3 PSAP for the EIDO by including the URI provided in the Call-Info header in Step 32 in a GET request.

**Step 38.** The transfer-from PSAP returns the EIDO to the transfer-to i3 PSAP.

**Step 39.** The transfer-to i3 PSAP accepts the invitation to the conference by returning a 200 OK message to the conferencing AS/MRFC (via the IBCF/Transit Function [not shown]).

*Note that Step 39 may happen before Steps 37 and 38. Acceptance of the invitation is not dependent on retrieval of the EIDO.*

**Step 40.** The conferencing AS/MRFC acknowledges receipt of the 200 OK message by returning an ACK.

*A media session is established between the transfer-to i3 PSAP and the conferencing AS/MRFC.*

**Step 41.** The conferencing AS/MRFC returns a NOTIFY message to the transfer-from i3 PSAP (via an IBCF [not shown]) to provide updated status of the subscription associated with the REFER request.

**Step 42.** The transfer-from i3 PSAP responds to the NOTIFY message by returning a 200 OK message.

**Step 43.** The transfer-to i3 PSAP subscribes to the conference associated with the Conf-ID provided in the INVITE message from the conferencing AS/MRFC by sending a SUBSCRIBE message to the I-CSCF (via the IBCF [not shown]).

**Step 44.** The I-CSCF passes the SUBSCRIBE message to the conferencing AS/MRFC.

**Step 45.** The conferencing AS/MRFC acknowledges the subscription request by sending a 200 OK message back to the I-CSCF.

**Step 46.** The I-CSCF passes the 200 OK message back to the transfer-to i3 PSAP (via the IBCF [not shown]).

**Step 47.** The conferencing AS/MRFC then returns a NOTIFY message to the transfer-to i3 PSAP (via the IBCF [not shown]) to provide subscription status information.

**Step 48.** The transfer-to i3 PSAP responds by returning a 200 OK message.

**Step 49.** The conferencing AS/MRFC sends a NOTIFY message to the transfer-from i3 PSAP (via an IBCF [not shown]) providing updated status for the subscription associated with the REFER request.

**Step 50.** The transfer-from i3 PSAP responds to the NOTIFY message by returning a 200 OK message.

*At this point the caller, transfer-from i3 PSAP, and transfer-to i3 PSAP are all participants in the conference.*

### 8.8.1.1.3.2 Transfer-to PSAP is a Legacy PSAP

Figure 8-22 illustrates a scenario where the transfer-to PSAP is a legacy PSAP. (Note that all SIP messages between the Legacy PSAP Gateway and the conferencing AS/MRFC flow via an IBCF [not shown].)

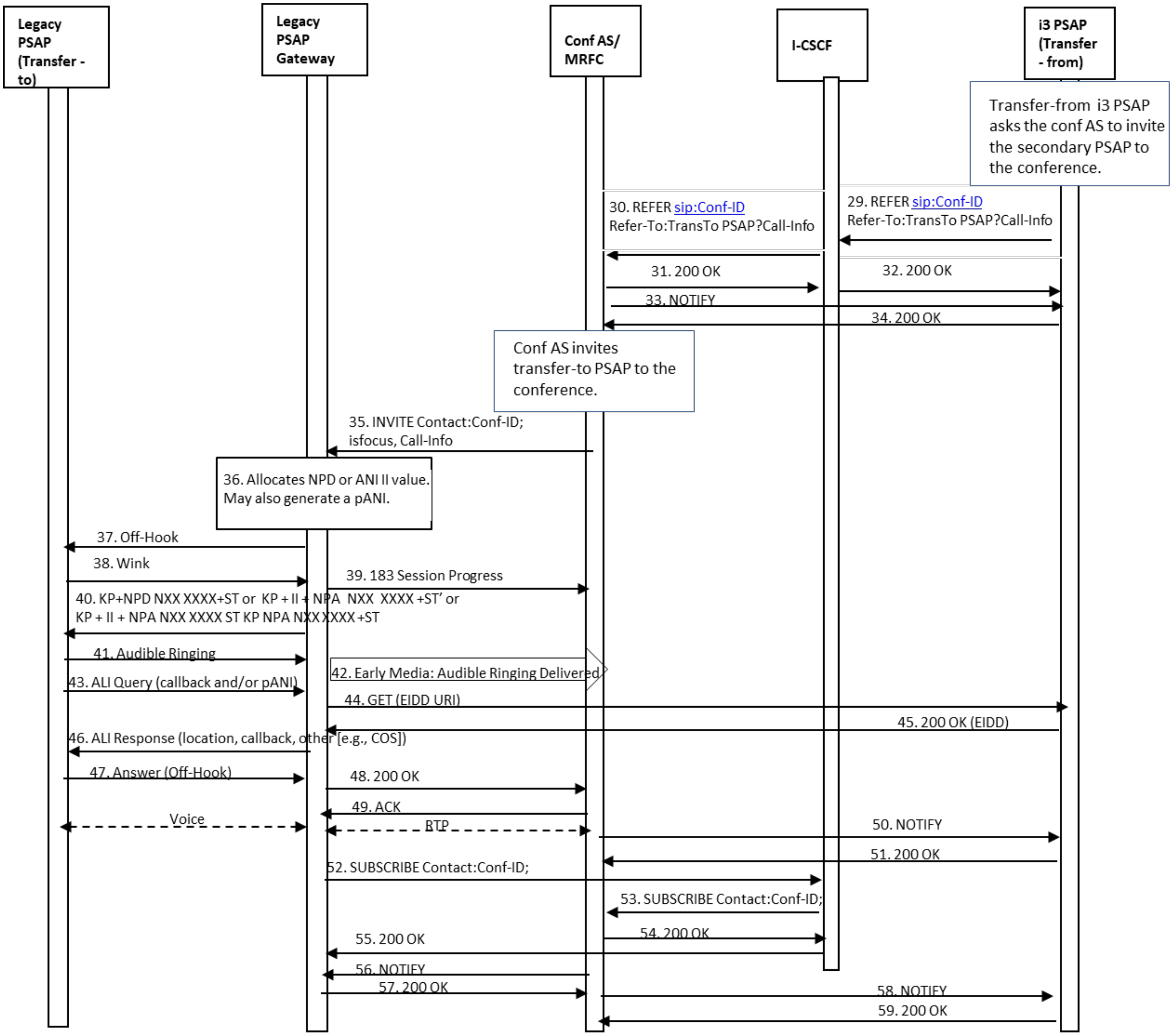

Legacy PSAP (Transfer - to)
Legacy PSAP Gateway
Conf AS/ MRFC
I-CSCF
i3 PSAP (Transfer - from)
Transfer-from i3 PSAP asks the conf AS to invite the secondary PSAP to the conference.
29. REFER sip:Conf-ID Refer-To:TransTo PSAP?Call-Info
30. REFER sip:Conf-ID Refer-To:TransTo PSAP?Call-Info
31. 200 OK
32. 200 OK
33. NOTIFY
34. 200 OK
Conf AS invites transfer-to PSAP to the conference.
35. INVITE Contact:Conf-ID; isfocus, Call-Info
36. Allocates NPD or ANI II value. May also generate a pANI.
37. Off-Hook
38. Wink
39. 183 Session Progress
40. KP+NPD NXX XXXX+ST or KP + II + NPA NXX XXXX +ST' or KP + II + NPA NXX XXXX ST KP NPA NXX XXXX +ST
41. Audible Ringing
42. Early Media: Audible Ringing Delivered
43. ALI Query (callback and/or pANI)
44. GET (EIDD URI)
45. 200 OK (EIDD)
46. ALI Response (location, callback, other [e.g., COS])
47. Answer (Off-Hook)
48. 200 OK
49. ACK
Voice
RTP
50. NOTIFY
51. 200 OK
52. SUBSCRIBE Contact:Conf-ID;
53. SUBSCRIBE Contact:Conf-ID;
54. 200 OK
55. 200 OK
56. NOTIFY
57. 200 OK
58. NOTIFY
59. 200 OK

**Figure 8.24: i3 PSAP Requests that a Transfer-to Legacy PSAP be Invited to the Conference**

**Step 29.** The transfer-from i3 PSAP sends a REFER method I-CSCF (via an IBCF [not shown]).

**Step 30.** The I-CSCF passes the REFER method to the conferencing AS/MRFC. The I-CSCF does not add itself to the Record-Route header since it does not need to remain in the signaling path for subsequent requests. The REFER method requests that the conferencing AS/MRFC invite the transfer-to (legacy) PSAP to the conference. The REFER method contains the Conf-ID and a Refer-To header that contains the URI of the transfer-to (legacy) PSAP. The REFER method also contains an escaped Call-Info header field containing a reference URI that points to the EIDO data structure and a purpose parameter of “eido”.

**Step 31.** The conferencing AS/MRFC returns a 200 OK message to the I-CSCF.

**Step 32.** The I-CSCF passes the 200 OK message (via an IBCF [not shown]) to the transfer-from i3 PSAP.

**Step 33.** The conferencing AS/MRFC then returns a NOTIFY message (via an IBCF [not shown]), indicating that subscription state of the REFER request (i.e., active).

**Step 34.** The transfer-from i3 PSAP returns a 200 OK message to the conferencing AS/MRFC (via an IBCF [not shown]) in response to the NOTIFY message.

**Step 35.** The conferencing AS/MRFC invites the transfer-to (legacy) PSAP to the conference by sending an INVITE method (via a Transit Function/IBCF [not shown]) containing the Conf-ID and Contact header that contains the conference URI and the isfocus feature parameter to the LPG. The INVITE also contains the Call-Info header field containing a reference URI that points to the EIDO data structure and a purpose parameter of “eido”. The SIP INVITE message will include a Resource Priority Header set to “esnet.1” to indicate that the session request is associated with the transfer of an emergency call.

**Step 36.** The LPG determines, based on provisioning, whether the transfer-to PSAP supports a Traditional MF or Enhanced MF interface. Depending on the type of interface supported by the PSAP, the LPG may generate a pANI and will assign an appropriate NPD or ANI II value to the call, following the procedures specified in Clause 6.2.2 of NENA-STA-010.3 [Ref 27].

**Step 37.** The LPG generates an off-hook signal toward the legacy PSAP.

**Step 38.** The legacy PSAP returns a wink signal back to the LPG.

**Step 39.** The LPG generates a 183 Session Progress message and sends it to the conferencing AS/MRFC (via the IBCF/Transit Function [not shown]).

**Step 40.** The LPG delivers the call to the legacy PSAP, mapping the SIP signaling from the incoming INVITE message to the outgoing Traditional or Enhanced MF signaling sequences, as appropriate for the legacy PSAP.

**Step 41.** Audible ringing is returned by the legacy PSAP to the LPG.

**Step 42.** Audible ringing is passed by the LPG to the conferencing AS/MRFC.

**Step 43.** The legacy PSAP sends a location query to the LPG using a legacy ALI protocol.

**Step 44.** The LPG queries the transfer-from i3 PSAP for the EIDO by including the URI provided in the Call-Info header in Step 32 in a GET request.

**Step 45.** The transfer-from PSAP returns the EIDO to the LPG.

**Step 46.** The LPG returns an ALI response to the legacy PSAP that includes the initial caller location information, a callback number and other information (e.g., class of service), as appropriate for the interface.

**Step 47.** When the PSAP answers the call, it returns an off-hook signal to the LPG.

**Step 48.** The LPG accepts the invitation to the conference by returning a 200 OK message to the conferencing AS/MRFC (via the IBCF/Transit Function [not shown]).

**Step 49.** The conferencing AS/MRFC acknowledges receipt of the 200 OK message by returning an ACK.

*A media session is established between the transfer-to (legacy) PSAP and the conferencing AS/MRFC.*

**Step 50.** The conferencing AS/MRFC returns a NOTIFY message to the transfer-from i3 PSAP (via an IBCF [not shown]) to provide updated status of the subscription associated with the REFER request.

**Step 51.** The transfer-from i3 PSAP responds to the NOTIFY message by returning a 200 OK message.

**Step 52.** The LPG subscribes to the conference associated with the Conf-ID provided in the INVITE message from the conferencing AS/MRFC by sending a SUBSCRIBE message to the I-CSCF.

**Step 53.** The I-CSCF passes the SUBSCRIBE message to the conferencing AS/MRFC (via the IBCF [not shown]).

**Step 54.** The conferencing AS/MRFC acknowledges the subscription request by sending a 200 OK message back to the I-CSCF.

**Step 55.** The I-CSCF passes the 200 OK message to the LPG (via the IBCF [not shown]).

**Step 56.** The conferencing AS/MRFC then returns a NOTIFY message to the LPG (via the IBCF [not shown]) to provide subscription status information.

**Step 57.** The LPG responds by returning a 200 OK message.

**Step 58.** The conferencing AS/MRFC sends a NOTIFY message to the transfer-from i3 PSAP (via an IBCF [not shown]), providing updated status for the subscription associated with the REFER request.

**Step 59.** The transfer-from i3 PSAP responds to the NOTIFY message by returning a 200 OK message.

*At this point the caller, transfer-from i3 PSAP, and transfer-to i3 PSAP are all participants in the conference.*

### 8.8.1.1.4 Transfer-from i3 PSAP Disconnects from the Conference

Once the transfer-from i3 PSAP determines that the transfer can be completed, the transfer-from i3 PSAP disconnects from the conference, as illustrated in Figure 8-23 and Figure 8-24.

### 8.8.1.1.4.1 Transfer-to PSAP is an i3 PSAP

This call flow illustrates a scenario when the transfer-to PSAP is an i3 PSAP.

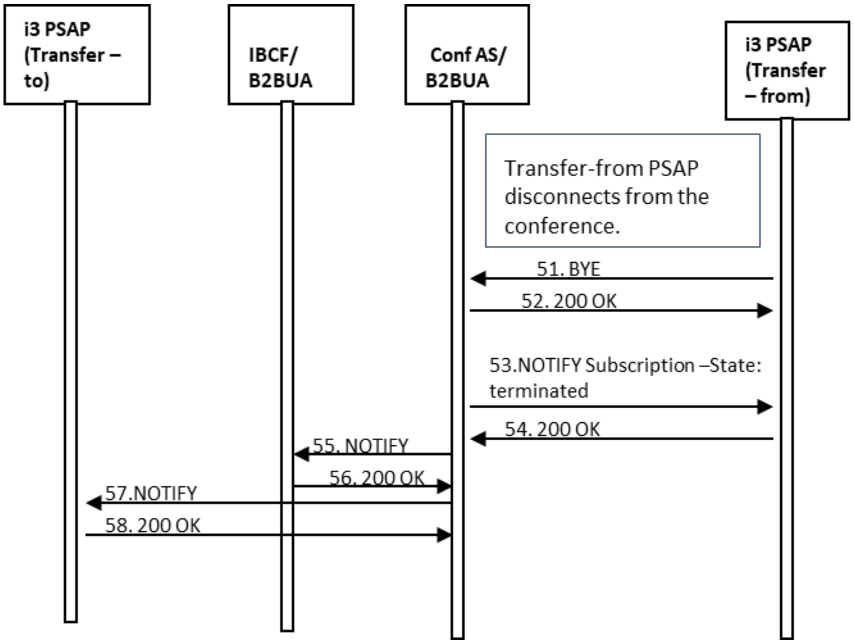

i3 PSAP (Transfer – to)
IBCF/ B2BUA
Conf AS/ B2BUA
i3 PSAP (Transfer – from)
Transfer-from PSAP disconnects from the conference.
51. BYE
52. 200 OK
53.NOTIFY Subscription –State: terminated
54. 200 OK
55. NOTIFY
56. 200 OK
57.NOTIFY
58. 200 OK

**Figure 8.25: Transfer-from i3 PSAP Disconnects from the Conference – Transfer-to PSAP is an I3 PSAP**

**Step 51.** Upon determining that the emergency call transfer should be completed, the transfer-from PSAP disconnects from the call by sending a BYE message to the conferencing AS/MRFC (via an IBCF [not shown]).

**Step 52.** The conferencing AS/MRFS responds by returning a 200 OK message.

**Step 53.** The conferencing AS/MRFC then returns a NOTIFY message to the transfer-from i3 PSAP (via an IBCF [not shown]) indicating that the subscription to the conference has been terminated.

**Step 54.** The transfer-from i3 PSAP returns a 200 OK message in response to the NOTIFY message.

**Step 55.** The conferencing AS/MRFC then returns a NOTIFY message to the IBCF/B2BUA indicating that there has been a change to the subscription state.

**Step 56.** The IBCF/B2BUA returns a 200 OK message in response to the NOTIFY message.

**Step 57.** The conferencing AS/MRFC then returns a NOTIFY message to the transfer-to i3 PSAP (via the IBCF [not shown]) indicating that there has been a change to the subscription state.

**Step 58.** The transfer-to i3 PSAP returns a 200 OK message in response to the NOTIFY message.

### 8.8.1.1.4.2 Transfer-to PSAP is a Legacy PSAP

This call flow illustrates a scenario when the transfer-to PSAP is a legacy PSAP.

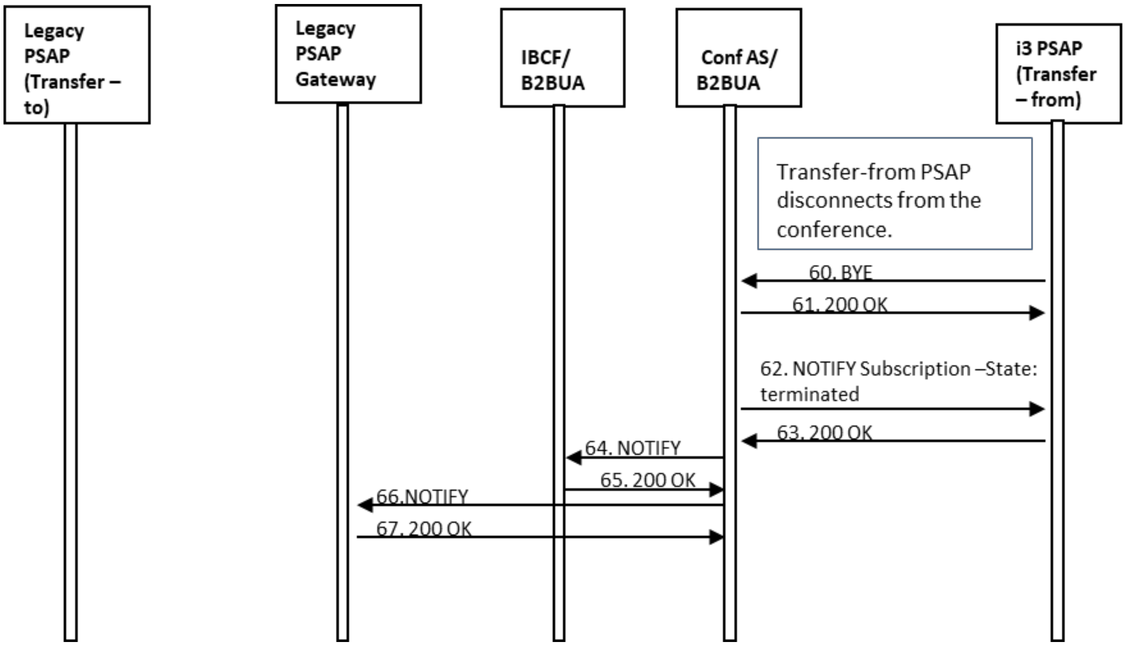

Legacy PSAP (Transfer – to)
Legacy PSAP Gateway
IBCF/ B2BUA
Conf AS/ B2BUA
i3 PSAP (Transfer – from)
Transfer-from PSAP disconnects from the conference.
60. BYE
61. 200 OK
62. NOTIFY Subscription –State: terminated
63. 200 OK
64. NOTIFY
65. 200 OK
66.NOTIFY
67. 200 OK

**Figure 8.26: Transfer-from i3 PSAP Disconnects from the Conference – Transfer-to PSAP is a Legacy PSAP**

**Step 60.** Upon determining that the emergency call transfer should be completed, the transfer-from PSAP disconnects from the call by sending a BYE message to the conferencing AS/MRFC (via the IBCF [not shown]).

**Step 61.** The conferencing AS/MRFS responds by returning a 200 OK message.

**Step 62.** The conferencing AS/MRFC then returns a NOTIFY message to the transfer-from i3 PSAP (via the IBCF [not shown]) indicating that the subscription to the conference has been terminated.

**Step 63.** The transfer-from i3 PSAP returns a 200 OK message in response to the NOTIFY message.

**Step 64.** The conferencing AS/MRFC then returns a NOTIFY message to the IBCF/B2BUA indicating that there has been a change to the subscription state.

**Step 65.** The IBCF/B2BUA returns a 200 OK message in response to the NOTIFY message.

**Step 66.** The conferencing AS/MRFC then returns a NOTIFY message to the LPG (via the IBCF [not shown]) indicating that there has been a change to the subscription state.

**Step 67.** The LPG returns a 200 OK message in response to the NOTIFY message.

### 8.8.1.1.5 Transfer-to PSAP Completes the Transfer

The transfer-to PSAP then completes the transfer as illustrated in Figure 8-25 and Figure 8-26. Note that the connection between the caller and the IBCF/B2BUA is unaffected by the completion of the transfer by the transfer-to PSAP. The following flows also illustrate termination of the emergency call initiated by the transfer-to PSAP.

#### 8.8.1.1.5.1 Transfer-to PSAP is an i3 PSAP

This call flow illustrates a scenario when the transfer-to PSAP is an i3 PSAP.

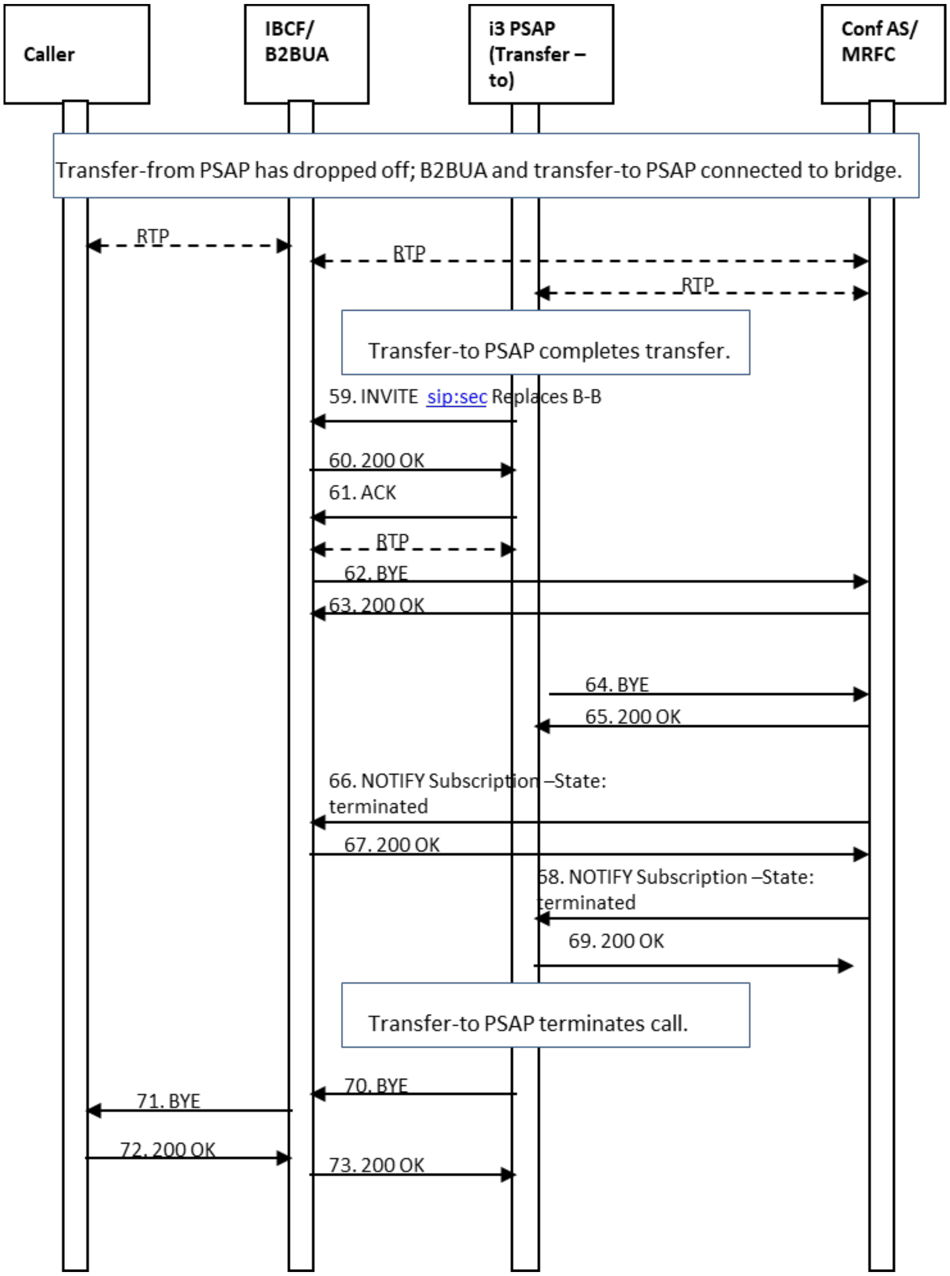

Caller
IBCF/ B2BUA
i3 PSAP (Transfer – to)
Conf AS/ MRFC
Transfer-from PSAP has dropped off; B2BUA and transfer-to PSAP connected to bridge.
RTP
RTP
RTP
Transfer-to PSAP completes transfer.
59. INVITE sip:sec Replaces B-B
60. 200 OK
61. ACK
RTP
62. BYE
63. 200 OK
64. BYE
65. 200 OK
66. NOTIFY Subscription –State: terminated
67. 200 OK
68. NOTIFY Subscription –State: terminated
69. 200 OK
Transfer-to PSAP terminates call.
70. BYE
71. BYE
72. 200 OK
73. 200 OK

**Figure 8.27: Transfer-to i3 PSAP Completes the Transfer and Terminates the Call**

**Step 59.** The transfer-to i3 PSAP completes the transfer by sending a SIP INVITE message to the IBCF/B2BUA requesting that it replaces its connection to the conferencing AS/MRFC with a direct connection to the transfer-to i3 PSAP. (The transfer-to i3 PSAP learns the URI of the IBCF/B2BUA from the ‘entity’ attribute, and the call-id from the <call-info> child element of the <endpoint> portion of the <user> sub-element in the <conference-info> with the NOTIFY message from the bridge. See RFC 4575 [Ref 31] for further details.)

**Step 60.** The IBCF/B2BUA responds by returning a 200 OK message.

**Step 61.** The transfer-to i3 PSAP returns an ACK in response to the 200 OK message.

*At this point, a session is established between the IBCF/B2BUA and the transfer-to i3 PSAP. The media session between the IBCF/B2BUA and the conferencing AS/MRFC also still exists at this time.*

**Step 62.** The IBCF/B2BUA then sends a BYE to the conferencing AS/MRFC to terminate the session.

*At this point, the IBCF/B2BUA switches the media from the session with the conferencing AS/MRFC to the session with the transfer-to PSAP.*

**Step 63.** The conferencing AS/MRFC responds by returning a 200 OK message.

*At this time the session between the B2BUA and the conferencing AS/MRFC is terminated.*

**Step 64.** The transfer-to i3PSAP also terminates its session with the conferencing AS/MRFC by sending a BYE message (via an IBCF) to the conferencing AS/MRFC.

*At this point, the transfer-to PSAP switches the media from the session with the conferencing AS/MRFC to the session with the IBCF/B2BUA.*

**Step 65.** The conferencing AS/MRFC responds by sending a 200 OK message to the transfer-to i3 PSAP.

*At this point, the session between the transfer-to i3 PSAP and the conferencing AS/MRFC is terminated.*

**Step 66.** The conferencing AS/MRFC then returns a NOTIFY message to the IBCF/B2BUA indicating that the subscription to the conference has been terminated.

**Step 67.** The IBCF/B2BUA responds with a 200 OK message.

**Step 68.** The conferencing AS/MRFC then returns a NOTIFY message to the transfer-to i3 PSAP (via an IBCF [not shown]) indicating that the subscription to the conference has been terminated.

**Step 69.** The transfer-to i3 PSAP responds with a 200 OK message.

*At this point, the transfer is complete. The caller and the transfer-to PSAP are involved in a two-way call.*

**Step 70.** The transfer-to i3 PSAP determines that the call should be terminated and sends a BYE message (via an IBCF [not shown]) to the IBCF/B2BUA.

**Step 71.** The IBCF/B2BUA sends a BYE message to the calling device to terminate the session.

**Step 72.** The calling device sends a 200 OK message to the B2BUA in response to the BYE.

**Step 73.** The IBCF/B2BUA sends a 200 OK message to the transfer-to i3 PSAP (via an IBCF [not shown]) in response to receiving the 200 OK message from the calling device.

*At this point the emergency session is terminated.*

### 8.8.1.1.5.2 Transfer-to PSAP is a Legacy PSAP

This call flow illustrates a scenario when the transfer-to PSAP is a legacy PSAP.

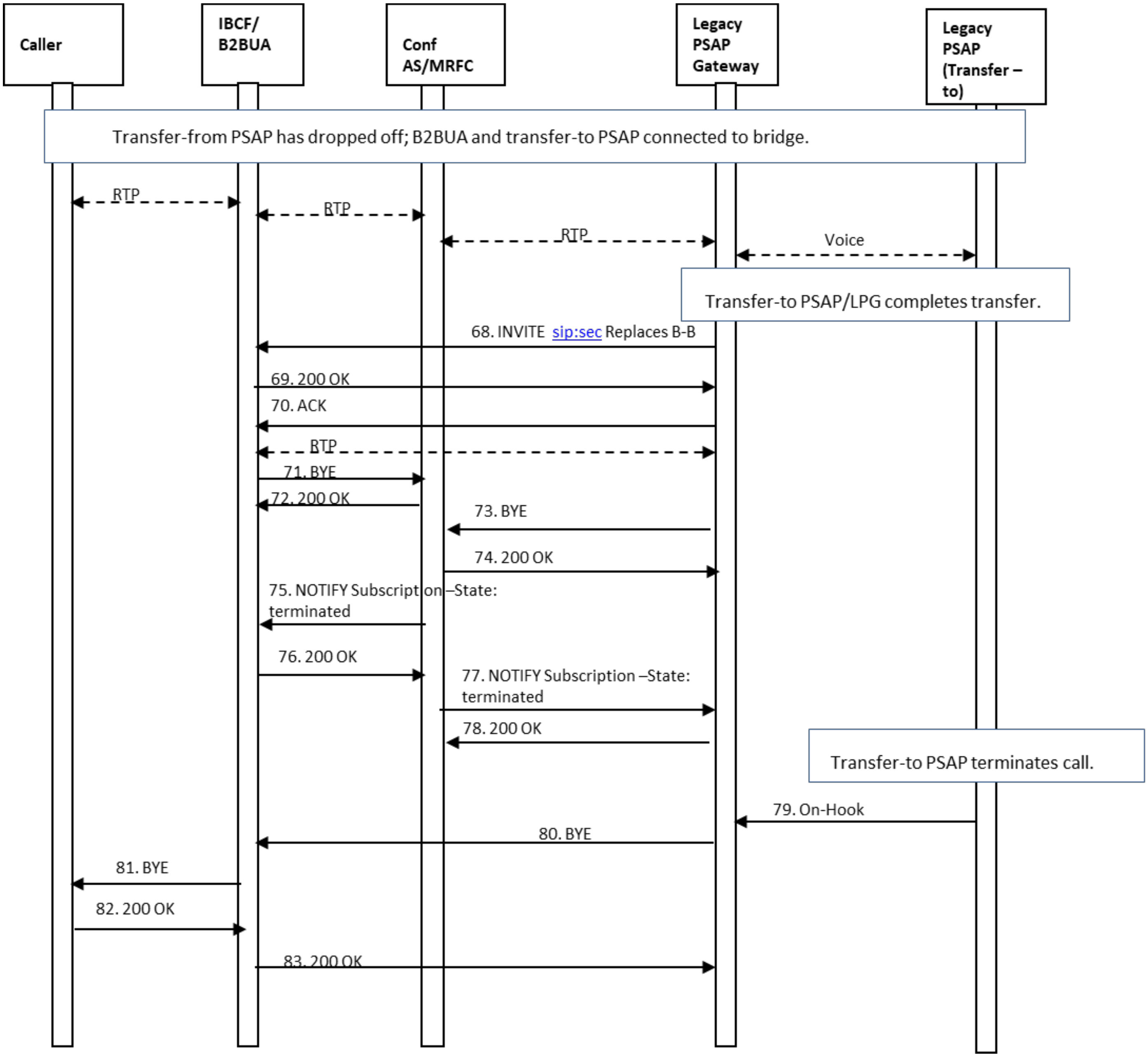

Caller
IBCF/ B2BUA
Conf AS/MRFC
Legacy PSAP Gateway
Legacy PSAP (Transfer – to)
Transfer-from PSAP has dropped off; B2BUA and transfer-to PSAP connected to bridge.
RTP
RTP
RTP
Voice
Transfer-to PSAP/LPG completes transfer.
68. INVITE sip:sec Replaces B-B
69. 200 OK
70. ACK
RTP
71. BYE
72. 200 OK
73. BYE
74. 200 OK
75. NOTIFY Subscription –State: terminated
76. 200 OK
77. NOTIFY Subscription –State: terminated
78. 200 OK
Transfer-to PSAP terminates call.
79. On-Hook
80. BYE
81. BYE
82. 200 OK
83. 200 OK

**Figure 8.28: Transfer-to Legacy PSAP/LPG Completes the Transfer and Terminates the Call**

**Step 68.** The LPG completes the transfer by sending a SIP INVITE message to the IBCF/B2BUA requesting that it replaces its connection to the conferencing AS/MRFC with a direct connection to the LPG. (The LPG learns the URI of the IBCF/B2BUA from the 'entity' attribute, and the call-id from the <call-info> child element of the <endpoint> portion of the <user> sub-element in the <conference-info> within the NOTIFY message from the bridge. See RFC 4575 [Ref 31] for further details.)

**Step 69.** The IBCF/B2BUA responds by returning a 200 OK message.

**Step 70.** The LPG returns an ACK in response to the 200 OK message.

*At this point, a session is established between the IBCF/B2BUA and the transfer-to legacy PSAP via the LPG. The media session between the IBCF/B2BUA and the conferencing AS/MRFC also still exists at this time.*

**Step 71.** The IBCF/B2BUA then sends a BYE to the conferencing AS/MRFC to terminate the session.

*At this point, the IBCF/B2BUA switches the media from the session with the conferencing AS/MRFC to the session with the LPG/transfer-to PSAP.*

**Step 72.** The conferencing AS/MRFC responds by returning a 200 OK message.

*At this time the session between the IBCF/B2BUA and the conferencing AS/MRFC is terminated.*

**Step 73.** The LPG also terminates its session with the conferencing AS/MRFC by sending a BYE message to the conferencing AS/MRFC (via an IBCF [not shown]).

*At this point, the LPG switches the media from the session with the conferencing AS/MRFC to the session with the IBCF/B2BUA.*

**Step 74.** The conferencing AS/MRFC responds by sending a 200 OK message to the LPG (via an IBCF [not shown]).

*At this point, the session between the LPG and the conferencing AS/MRFC is terminated.*

**Step 75.** The conferencing AS/MRFC then returns a NOTIFY message to the IBCF/B2BUA indicating that the subscription to the conference has been terminated.

**Step 76.** The IBCF/B2BUA responds with a 200 OK message.

**Step 77.** The conferencing AS/MRFC then returns a NOTIFY message to the LPG (via an IBCF [not shown]) indicating that the subscription to the conference has been terminated.

**Step 78.** The LPG responds with a 200 OK message.

*At this point, the transfer is complete. The caller and the transfer-to PSAP are involved in a two-way call.*

**Step 79.** The transfer-to (legacy) PSAP determines that the call should be terminated and sends an on-hook indication to the LPG.

**Step 80.** The LPG maps the on-hook indication to a SIP BYE message and sends the SIP BYE message (via an IBCF [not shown]) to the IBCF/B2BUA.

**Step 81.** The IBCF/B2BUA sends a BYE message to the calling device to terminate the session.

**Step 82.** The calling device sends a 200 OK message to the B2BUA in response to the BYE.

**Step 83.** The IBCF/B2BUA sends a 200 OK message to the LPG (via an IBCF [not shown]) in response to receiving the 200 OK message from the calling device.

*At this point the emergency session is terminated.*

### 8.8.1.2 Signaling/Media Anchoring at Egress Point

This clause illustrates the call flow where the header replacement and media anchoring happens at the PSAP-facing IBCF. The E-CSCF in the emergency network will route the call to an IBCF that would be used as B2BUA for media anchoring. The role played by the originating network-facing IBCF can be either a B2BUA or Proxy.

The initial call is established and is shown as call #1 between IBCFs, and call #1a between IBCF#2 and the transfer-from PSAP. The PSAP (referred to as transfer-from PSAP and is shown as transfer-from PSAP) transfers the emergency call to a transfer-to PSAP. Before the transfer, the transfer-from PSAP establishes a conference call between the emergency call originator and the transfer-to PSAP, and then drops out of the call to do the transfer. The overall process is executed in multiple steps.

#### 8.8.1.2.1 Transfer-from PSAP Requests the AS/MRFC to Invoke the Conference

In the first step, the transfer-from PSAP invokes the conference. The flow assumes that an emergency call is already established between the calling party and the transfer-from PSAP.

> NOTE: IBCF#2 and IBCF#3 may actually be the same physical IBCF but are shown separately to illustrate that it does not necessarily need to be the same.

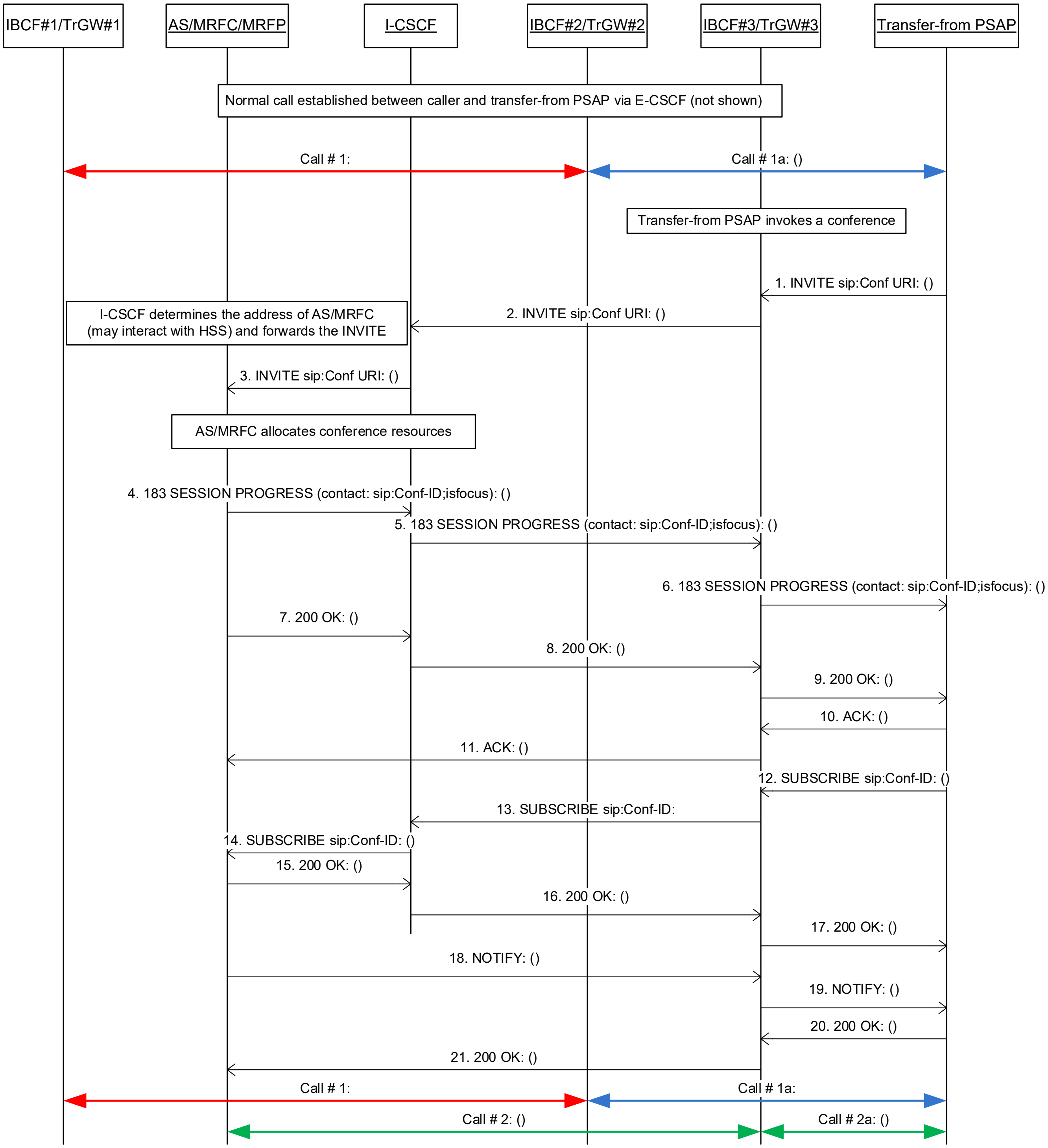

IBCF#1/TrGW#1
AS/MRFC/MRFP
I-CSCF
IBCF#2/TrGW#2
IBCF#3/TrGW#3
Transfer-from PSAP
Normal call established between caller and transfer-from PSAP via E-CSCF (not shown)
Call # 1:
Call # 1a: ()
Transfer-from PSAP invokes a conference
1. INVITE sip:Conf URI: ()
I-CSCF determines the address of AS/MRFC (may interact with HSS) and forwards the INVITE
2. INVITE sip:Conf URI: ()
3. INVITE sip:Conf URI: ()
AS/MRFC allocates conference resources
4. 183 SESSION PROGRESS (contact: sip:Conf-ID;isfocus): ()
5. 183 SESSION PROGRESS (contact: sip:Conf-ID;isfocus): ()
6. 183 SESSION PROGRESS (contact: sip:Conf-ID;isfocus): ()
7. 200 OK: ()
8. 200 OK: ()
9. 200 OK: ()
10. ACK: ()
11. ACK: ()
12. SUBSCRIBE sip:Conf-ID: ()
13. SUBSCRIBE sip:Conf-ID:
14. SUBSCRIBE sip:Conf-ID: ()
15. 200 OK: ()
16. 200 OK: ()
17. 200 OK: ()
18. NOTIFY: ()
19. NOTIFY: ()
20. 200 OK: ()
21. 200 OK: ()
Call # 1:
Call # 1a:
Call # 2: ()
Call # 2a: ()

**Figure 8.29: Transfer-from i3 PSAP Invokes the Conference**

**Step 1.** The transfer-from PSAP sends an INVITE with conference URI as the Request URI to the IBCF#3.

**Step 2.** The IBCF#3 forwards the INVITE to the I-CSCF.

**Step 3.** The I-CSCF determines the address of the conferencing AS/MRFC and forwards the INVITE to AS/MRFC.

NOTE: I-CSCF does not add itself to the Record-Route header.

**Step 4.** The conferencing AS/MRFC allocates a conference URI, based on local information, information gained from the conference-factory URI, and other information received in SIP signaling. The conferencing AS/MRFC responds to the INVITE by returning a 183 SESSION PROGRESS to the I-CSCF. The Contact header contains the conference URI for the conference allocated at the AS/MRFC and the “isfocus” feature parameter indicating a conference call.

**Step 5.** The I-CSCF forwards the 183 SESSION PROGRESS to the IBCF#3.

**Step 6.** The IBCF#3 forwards the 183 SESSION PROGRESS to the transfer-from PSAP.

**Step 7.** The AS/MRFC sends a 200 OK to the I-CSCF in response to the INVITE message.

**Step 8.** The I-CSCF forwards the 200 OK to the IBCF#3.

**Step 9.** The IBCF#3 forwards the 200 OK to the transfer-from PSAP.

**Step 10.** The transfer-from PSAP returns an ACK acknowledging the receipt of 200 OK to the IBCF#3.

**Step 11.** The IBCF#3 forwards the ACK to the AS/MRFC.

*At this point the media session is established between MRFP and the transfer-from PSAP. (The actual media leg between MRFP and IBCF#3 is denoted as call #2, and the media between IBCF#3 and the transfer-from PSAP is denoted as call #2a. The UE is still connected to the transfer-from PSAP as call #1.)*

**Step 12.** The transfer-from PSAP sends a SUBSCRIBE to AS/MRFC to stay informed regarding the status of the conference call to the IBCF#3.

**Step 13.** The IBCF#3 forwards the SUBSCRIBE to the I-CSCF.

**Step 14.** The I-CSCF forwards the SUBSCRIBE to the AS/MRFC.

**Step 15.** The AS/MRFC sends a 200 OK back to the I-CSCF.

**Step 16.** The I-CSCF forwards the 200 OK to the IBCF#3.

**Step 17.** The IBCF#3 forwards the 200 OK to the transfer-from PSAP.

**Step 18.** The AS/MRFC sends a NOTIFY to the transfer-from PSAP via IBCF#3.

**Step 19.** The IBCF#3 forwards the NOTIFY to the transfer-from PSAP.

**Step 20.** The transfer-from PSAP sends a 200 OK back to the AS/MRFC in response to NOTIFY via IBCF#3.

**Step 21.** The IBCF#3 forwards the 200 OK to the AS/MRFC.

#### 8.8.1.2.2 Transfer-from PSAP Requests Conferencing AS Invite IBCF#2/B2BUA to Conference

This call flow shows the bridging of call #1 (original call) through the conference to call #2.

NOTE: IBCF#2 and IBCF#3 may actually be the same physical IBCF but are shown separately to illustrate that it does not necessarily need to be the same.

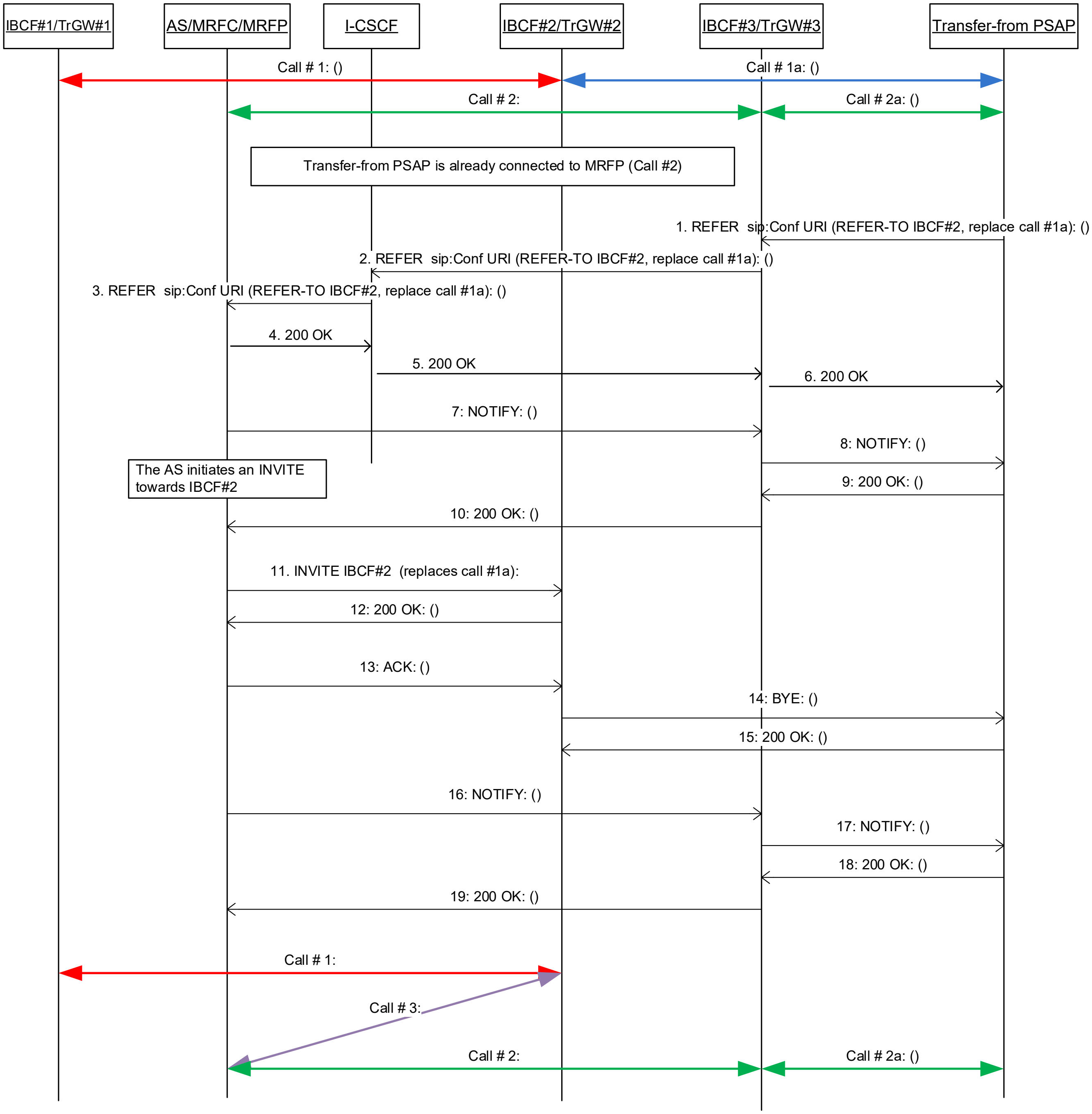


**Figure 8.30: Application Server (AS) Bridges Call #1 and Call #2 via IBCF#2**

**Step 1.** In order to bridge the original call with call #2 established with the AS/MRFC, call #1a needs to be redirected to the MRFP. The transfer-from PSAP sends a REFER to the IBCF#3 (with Request URI containing the Conference URI) with Refer-To header pointing to IBCF#2 and with Replaces identifying call #1a.

NOTE: REFER could go to a new IBCF instead of IBCF#3.

**Step 2.** The IBCF#3 forwards the REFER to the I-CSCF.

**Step 3.** The I-CSCF forwards the REFER to AS/MRFC. I-CSCF does not add itself to the Record-Route header.

**Step 4.** The AS/MRFC returns a 200 OK towards the transfer-from PSAP via I-CSCF.

**Step 5.** The I-CSCF forwards the 200 OK to the IBCF#3.

**Step 6.** The IBCF#3 forwards the 200 OK to the transfer-from PSAP.

**Step 7.** The AS/MRFC sends a NOTIFY towards the transfer-from PSAP via IBCF#3.

**Step 8.** The IBCF#3 forwards the NOTIFY to the transfer-from PSAP.

**Step 9.** The transfer-from PSAP responds back to the NOTIFY with a 200 OK.

**Step 10.** The IBCF#3 forwards the 200 OK to the AS/MRFC.

**Step 11.** The AS/MRFC initiates an INVITE towards IBCF#2; the Replaces in the INVITE identifies call #1a.

**Step 12.** The IBCF#2 sends a 200 OK back to the AS/MRFC.

**Step 13.** The AS/MRFC acknowledges the receipt of 200 OK by sending an ACK back to the IBCF#2.

**Step 14.** The IBCF#2 releases the connection for call #1a by sending a BYE towards the transfer-from PSAP.

*At this point, IBCF#2 switches the media from call #1a to call #3.*

**Step 15.** The transfer-from PSAP sends a 200 OK back to the IBCF#2.

*At this point, the transfer-from PSAP switches the media from call #1a to call #2.*

**Step 16.** The conference AS/MRFC sends a NOTIFY to the transfer-from PSAP via IBCF#3 to indicate that the session setup to IBCF#2 (as requested in the REFER) is completed.

**Step 17.** The IBCF#3 forwards the NOTIFY to the transfer-from PSAP.

**Step 18.** The transfer-from PSAP sends a 200 OK back to the AS/MRFC via IBCF#3.

**Step 19.** The IBCF#3 forwards the 200 OK to the AS/MRFC.

*At this point the original call (i.e., call #1) is connected to the new call #3 at IBCF#2/TrGW#2. Call #2 was created between the transfer-from PSAP and AS/MRFC/MRFP via IBCF#3/TrGW#3. Finally call #1a between IBCF#2 and the transfer-from PSAP is released.*

### 8.8.1.2.3 Transfer-from PSAP Requests that the Conferencing AS Invite the Transfer-to PSAP to the Conference

At this point the PSAP is communicating to the originating party through the conference. Then the transfer-from PSAP initiates a call to the transfer-to PSAP through the AS/MRFC. As described in Clause 8.8.1.1.3, the i3 PSAP will determine the URI associated with the transfer-to PSAP by querying an ECRF using a service URN in the "urn:emergency:service:responder" family and the location information received with the call (not shown in figures below). The i3 PSAP will use this URI to populate the Refer-To header of the outgoing REFER method. When the transfer-from PSAP handles a call, it develops information about the call that must be passed to subsequent PSAPs, dispatchers, and/or responders. This information is included in an Additional Data structure referred to as an Emergency Incident Data Object (EIDO). When the transfer-from PSAP requests an AS/MRFC to invite the transfer-to PSAP to the call, it must include all necessary call data for the call in the request.

#### 8.8.1.2.3.1 Transfer-to PSAP is an i3 PSAP

This call flow illustrates a scenario when the transfer-to PSAP is an i3 PSAP.

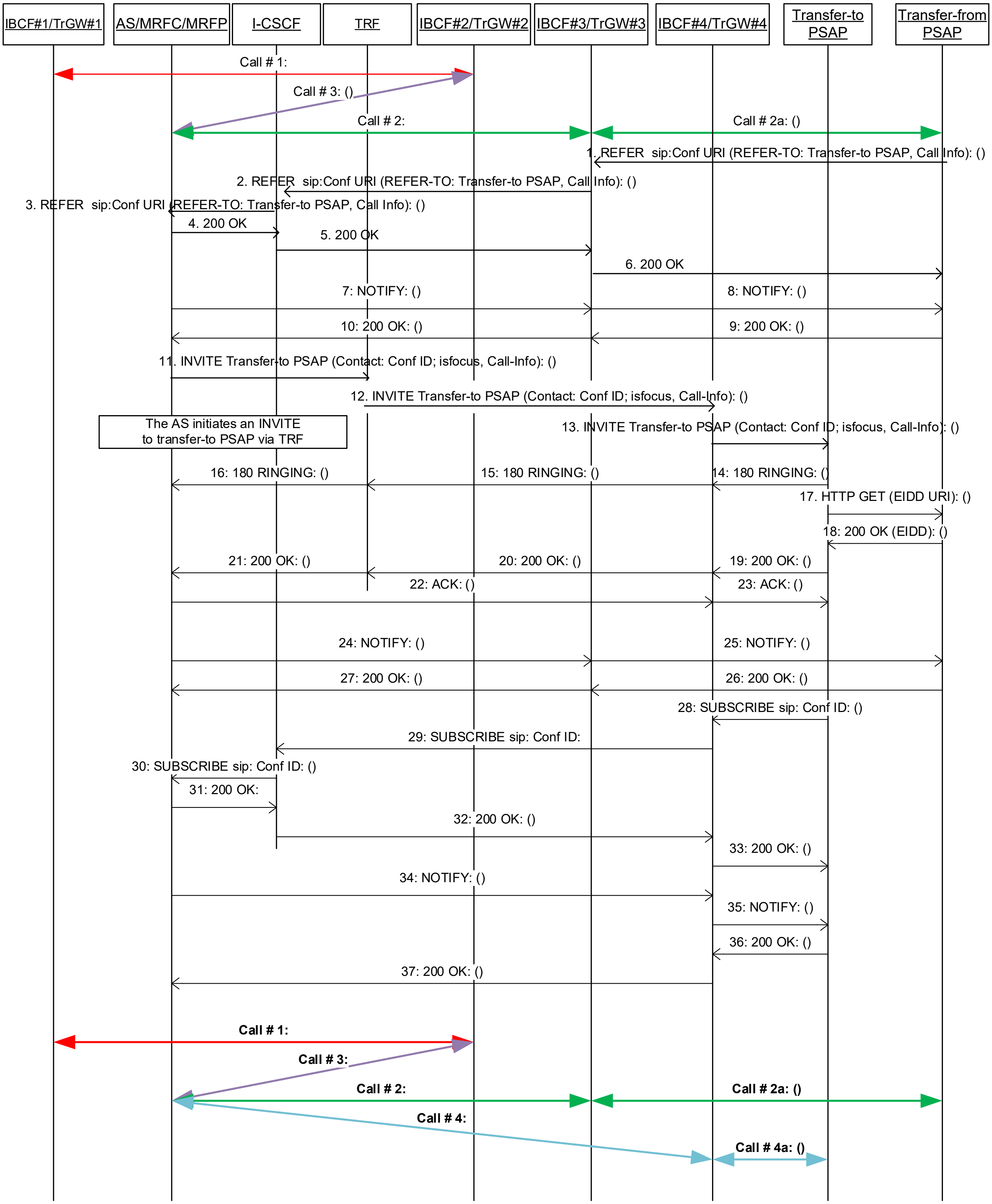


**Figure 8.31: Application Server (AS) Invites Transfer-to i3 PSAP to Conference**

**Step 1.** The transfer-from PSAP sends a REFER to the IBCF#3 (with Request URI containing the Conference URI) with Refer-To header pointing to transfer-to PSAP (shown as transfer-to PSAP). The REFER also contains an escaped Call-Info header containing a reference URI that points to the EIDO data structure and a purpose parameter of "eido".

**Step 2.** The IBCF#3 forwards the REFER to the I-CSCF to be forwarded to the AS/MRFC.

**Step 3.** The I-CSCF forwards the REFER to the AS/MRFC.

**Step 4.** The AS/MRFC sends a 200 OK back to the transfer-from PSAP via I-CSCF.

**Step 5.** The I-CSCF forwards the 200 OK towards the IBCF#3.

**Step 6.** The IBCF#3 forwards the 200 OK towards the transfer-from PSAP.

**Step 7.** The AS/MRFC sends a NOTIFY towards the transfer-from PSAP via IBCF#3.

**Step 8.** The IBCF#3 forwards the NOTIFY to the transfer-from PSAP.

**Step 9.** The transfer-from PSAP sends a 200 OK back to the AS/MRFC via IBCF#3.

**Step 10.** The IBCF#3 forwards the 200 OK to the AS/MRFC.

**Step 11.** The AS/MRFC initiates a call establishment towards the transfer-to PSAP by sending an INVITE via TRF including the conference URI, Call-Info header and isfocus feature parameter.

**Step 12.** The TRF forwards the INVITE to IBCF#4 for delivery to the transfer-to PSAP.

**Step 13.** The IBCF#4 forwards the INVITE to the transfer-to PSAP.

**Step 14.** The transfer-to PSAP UA responds by returning a 180 RINGING to the AS/MRFC via IBCF#4.

**Step 15.** The IBCF#4 forwards the 180 RINGING to the TRF.

**Step 16.** The TRF forwards the 180 RINGING to the AS/MRFC.

**Step 17.** The transfer-to PSAP sends an HTTP GET (EIDO) towards transfer-from PSAP to get the EIDO from the transfer-from PSAP.

**Step 18.** The transfer-from PSAP responds back with a 200 OK containing the EIDO.

**Step 19.** The transfer-to PSAP accepts the invitation by returning a 200 OK back to AS/MRFC via IBCF#4.

**Step 20.** The IBCF#4 forwards the 200 OK to the TRF.

**Step 21.** The TRF forwards the 200 OK to the AS/MRFC.

**Step 22.** The AS/MRFC acknowledges the 200 OK by sending an ACK back to the transfer-to PSAP via IBCF#4.

**Step 23.** The IBCF#4 forwards the ACK to the transfer-to PSAP.

*At this point a media path has been setup between the MRFP and the transfer-to PSAP denoted by call #4 in the call flow.*

**Step 24.** The AS/MRFC sends a NOTIFY towards the transfer-from PSAP via IBCF#3 to indicate that the session setup to the transfer-to PSAP (as requested in the REFER) is completed.

**Step 25.** The IBCF#3 forwards the NOTIFY to the transfer-from PSAP.

**Step 26.** The transfer-from PSAP sends a 200 OK back to the AS/MRFC.

**Step 27.** The IBCF#3 forwards the 200 OK to the AS/MRFC.

*At this point the original call (call #1) is connected to the conference (via call #3). The transfer-from PSAP is bridged in via call #2 and the transfer-to PSAP is bridged in via call #4 as shown in the figure.*

**Step 28.** The transfer-to PSAP sends a SUBSCRIBE towards AS/MRFC via IBCF#4 to subscribe to the conference events.

**Step 29.** The IBCF#4 forwards the SUBSCRIBE to the I-CSCF.

**Step 30.** The I-CSCF forwards the SUBSCRIBE to the AS/MRFC.

**Step 31.** The AS/MRFC sends a 200 OK in response to the SUBSCRIBE via the I-CSCF.

**Step 32.** The I-CSCF forwards the 200 OK to IBCF#4.

**Step 33.** The IBCF#4 forwards the 200 OK to the transfer-to PSAP.

**Step 34.** The AS/MRFC sends a NOTIFY to the transfer-to PSAP via IBCF#4.

**Step 35.** The IBCF#4 forwards the NOTIFY to the transfer-to PSAP.

**Step 36.** The transfer-to PSAP sends a 200 OK in response to the NOTIFY via IBCF#4 to the AS/MRFC.

**Step 37.** The IBCF#4 forwards the 200 OK to the AS/MRFC.

#### 8.8.1.2.3.2 Transfer-to PSAP is a Legacy PSAP

This call flow illustrates a scenario when the transfer-to PSAP is a legacy PSAP.

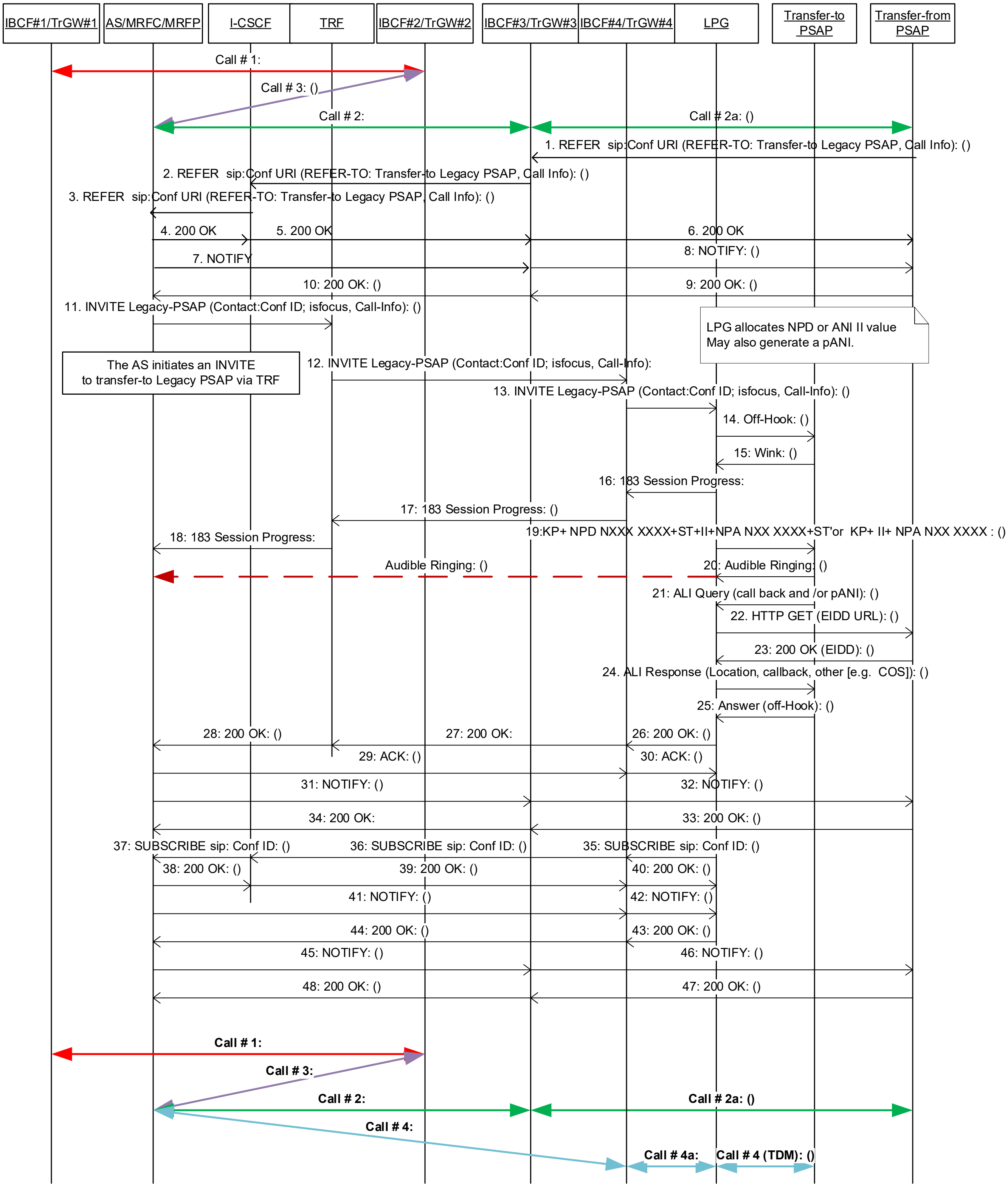

IBCF#1/TrGW#1
AS/MRFC/MRFP
I-CSCF
TRF
IBCF#2/TrGW#2
IBCF#3/TrGW#3
IBCF#4/TrGW#4
LPG
Transfer-to PSAP
Transfer-from PSAP
Call # 1:
Call # 3: ()
Call # 2:
Call # 2a: ()
1. REFER sip:Conf URI (REFER-TO: Transfer-to Legacy PSAP, Call Info): ()
2. REFER sip:Conf URI (REFER-TO: Transfer-to Legacy PSAP, Call Info): ()
3. REFER sip:Conf URI (REFER-TO: Transfer-to Legacy PSAP, Call Info): ()
4. 200 OK
5. 200 OK
6. 200 OK
7. NOTIFY
8: NOTIFY: ()
10: 200 OK: ()
9: 200 OK: ()
11. INVITE Legacy-PSAP (Contact:Conf ID; isfocus, Call-Info): ()
LPG allocates NPD or ANI II value
May also generate a pANI.
The AS initiates an INVITE
to transfer-to Legacy PSAP via TRF
12. INVITE Legacy-PSAP (Contact:Conf ID; isfocus, Call-Info):
13. INVITE Legacy-PSAP (Contact:Conf ID; isfocus, Call-Info): ()
14. Off-Hook: ()
15: Wink: ()
16: 183 Session Progress:
17: 183 Session Progress: ()
19:KP+ NPD NXXX XXXX+ST+II+NPA NXX XXXX+ST'or KP+ II+ NPA NXX XXXX : ()
18: 183 Session Progress:
Audible Ringing: ()
20: Audible Ringing: ()
21: ALI Query (call back and /or pANI): ()
22. HTTP GET (EIDD URL): ()
23: 200 OK (EIDD): ()
24. ALI Response (Location, callback, other [e.g. COS]): ()
25: Answer (off-Hook): ()
28: 200 OK: ()
27: 200 OK:
26: 200 OK: ()
29: ACK: ()
30: ACK: ()
31: NOTIFY: ()
32: NOTIFY: ()
34: 200 OK:
33: 200 OK: ()
37: SUBSCRIBE sip: Conf ID: ()
36: SUBSCRIBE sip: Conf ID: ()
35: SUBSCRIBE sip: Conf ID: ()
38: 200 OK: ()
39: 200 OK: ()
40: 200 OK: ()
41: NOTIFY: ()
42: NOTIFY: ()
44: 200 OK: ()
43: 200 OK: ()
45: NOTIFY: ()
46: NOTIFY: ()
48: 200 OK: ()
47: 200 OK: ()
Call # 1:
Call # 3:
Call # 2:
Call # 2a: ()
Call # 4:
Call # 4a:
Call # 4 (TDM): ()

**Figure 8.32: Application Server (AS) Invites Transfer-to Legacy PSAP to Conference**

**Step 1.** The transfer-from PSAP sends a REFER to the IBCF#3 (with Request URI containing the Conference URI) with Refer-To header pointing to the transfer-to PSAP (shown as Transfer-to PSAP). The REFER also contains an escaped Call-Info header containing a reference URI that points to the EIDO data structure and a purpose parameter of "eido".

**Step 2.** The IBCF#3 forwards the REFER to the I-CSCF to be forwarded to the AS/MRFC.

**Step 3.** The I-CSCF forwards the REFER to the AS/MRFC.

**Step 4.** The AS/MRFC sends a 200 OK back to the transfer-from PSAP via I-CSCF.

**Step 5.** The I-CSCF forwards the 200 OK towards the IBCF#3.

**Step 6.** The IBCF#3 forwards the 200 OK towards the transfer-from PSAP.

**Step 7.** The AS/MRFC sends a NOTIFY towards the transfer-from PSAP via IBCF#3.

**Step 8.** The IBCF#3 forwards the NOTIFY to the transfer-from PSAP.

**Step 9.** The transfer-from PSAP sends a 200 OK back to the AS/MRFC via IBCF#3.

**Step 10.** The IBCF#3 forwards the 200 OK to the AS/MRFC.

**Step 11.** The AS/MRFC initiates a call establishment towards the transfer-to PSAP by sending an INVITE towards the transfer-to PSAP via TRF including the conference URI, Call-Info header, and isfocus feature parameter.

**Step 12.** The TRF forwards the INVITE to the IBCF#4 for delivery to the transfer-to PSAP.

**Step 13.** The IBCF#4 forwards the INVITE to the LPG. The LPG determines, based on provisioning, whether the transfer-to PSAP supports a Traditional MF or Enhanced MF interface. Depending on the type of interface supported by the PSAP, the LPG may generate a pANI and will assign an appropriate NPD or ANI II value to the call, following the procedures specified in Clause 6.2.2 of NENA-STA-010.3 [Ref 27].

**Step 14.** The LPG generates an off-hook signal toward the legacy PSAP.

**Step 15.** The legacy PSAP returns a wink signal back to the LPG.

**Step 16.** The LPG generates a 183 Session Progress message and sends it to the conferencing AS/MRFC via the IBCF#4.

**Step 17.** The IBCF#4 forwards the 183 Session Progress message to the TRF.

**Step 18.** The TRF forwards the 183 Session Progress message to the AS/MRFC.

**Step 19.** The LPG delivers the call to the (transfer-to) legacy PSAP, mapping the SIP signaling from the incoming INVITE message to the outgoing Traditional or Enhanced MF signaling sequences, as needed for delivery to the legacy PSAP.

**Step 20.** The legacy PSAP returns with Audible ringing indication to the LPG. The LPG passes the Audible ringing indication to the AS/MRFC.

**Step 21.** The legacy PSAP sends a location query to the LPG using a legacy ALI protocol.

**Step 22.** The LPG queries the transfer-from i3 PSAP for the EIDO by including the URI provided in the Call-Info header in an outgoing GET request.

**Step 23.** The transfer-from PSAP returns the EIDO to the LPG in 200 OK.

**Step 24.** The LPG returns an ALI response to the (transfer-to) legacy PSAP that includes the initial caller location information, a callback number, and other information (e.g., class of service), as appropriate for the interface.

**Step 25.** When the transfer-to legacy PSAP answers the call, it returns an off-hook signal to the LPG.

**Step 26.** The LPG generates a 200 OK in response and sends it to the AS/MRFC via IBCF#4.

**Step 27.** The IBCF#4 forwards the 200 OK to the TRF.

**Step 28.** The TRF forwards the 200 OK to the AS/MRFC.

**Step 29.** The AS/MRFC sends an ACK back to the LPG via IBCF#4.

**Step 30.** The IBCF#4 forwards the ACK to the LPG.

**Step 31.** The AS/MRFC sends a NOTIFY towards the transfer-from PSAP via IBCF#3 to indicate that the session setup to the transfer-to PSAP (as requested in the REFER) is completed.

**Step 32.** The IBCF#3 forwards the NOTIFY to the transfer-from PSAP.

**Step 33.** The transfer-from PSAP sends a 200 OK back to the AS/MRFC via IBCF#3.

**Step 34.** The IBCF#3 forwards the 200 OK to the AS/MRFC. At this point the original call (call #1) is connected to the conference (via call #3). The transfer-from PSAP is bridged in via call #2, and the transfer-to PSAP is bridged in via call #4 as shown in the figure.

NOTE: The call #4 to the left of the LPG is an RTP based call, while to the right of the LPG is a TDM based call.

**Step 35.** The LPG sends a SUBSCRIBE towards AS/MRFC to subscribe to the conference events.

NOTE: The SUBSCRIBE message could go through a different IBCF than IBCF #4.

**Step 36.** The IBCF#4 forwards the SUBSCRIBE to the I-CSCF.

**Step 37.** The I-CSCF forwards the SUBSCRIBE to the AS/MRFC.

**Step 38.** The AS/MRFC sends a 200 OK in response via I-CSCF.

**Step 39.** The I-CSCF forwards the 200 OK to the IBCF#4.

**Step 40.** The IBCF#4 forwards the 200 OK to the LPG.

**Step 41.** The AS/MRFC sends a NOTIFY to the LPG via IBCF#4.

**Step 42.** The IBCF#4 forwards the NOTIFY to the LPG.

**Step 43.** The LPG sends a 200 OK in response to NOTIFY back towards AS/MRFC via IBCF#4.

**Step 44.** The IBCF#4 forwards the 200 OK to the AS/MRFC.

**Step 45.** The AS/MRFC sends a NOTIFY to the transfer-from PSAP via IBCF#3 providing an update on the conference events.

**Step 46.** The IBCF#3 forwards the NOTIFY to the transfer-from PSAP.

**Step 47.** The transfer-from PSAP sends 200 OK back to the AS/MRFC via IBCF#3 in response.

**Step 48.** The IBCF#3 forwards the 200 OK to the AS/MRFC.

### 8.8.1.2.4 Transfer i3 PSAP Disconnects from the Conference

After conferencing with the calling party and the transfer-to PSAP, the transfer-from PSAP wants the transfer-to PSAP to take over the handling of the call. The transfer-from PSAP drops out of the conference. This call flow illustrates the release of transfer-from PSAP from the call path.

#### 8.8.1.2.4.1 Transfer-to PSAP is an i3 PSAP

This call flow illustrates a call flow scenario where the transfer-to PSAP is an i3 PSAP.

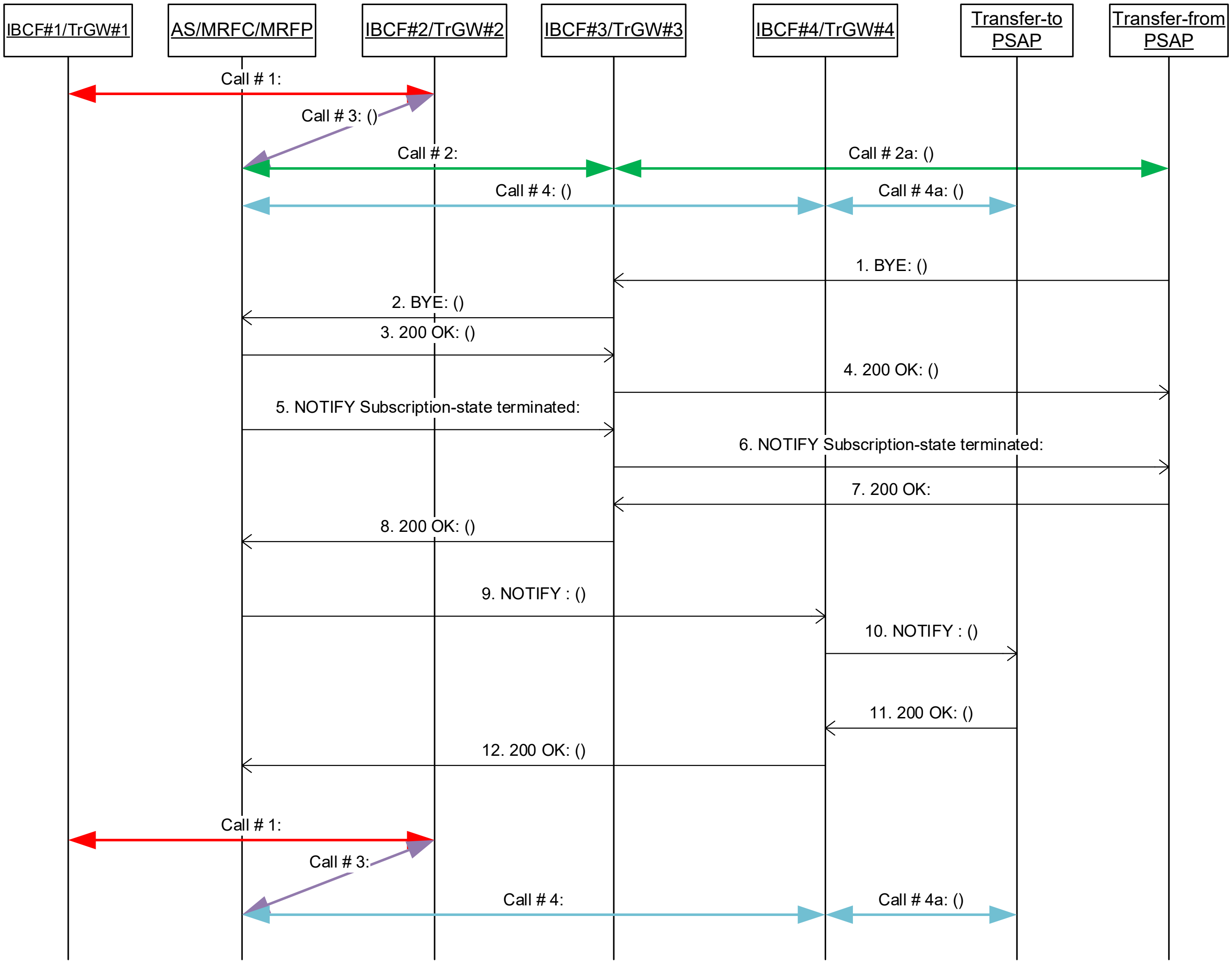


**Figure 8.33: Transfer-from i3 PSAP Drops out of Conference with Transfer-to i3 PSAP**

**Step 1.** The transfer-from PSAP initiates a BYE towards the AS/MRFC to disconnect itself from the call via IBCF#3.

**Step 2.** The BYE is forwarded to AS/MRFC by the IBCF#3.

**Step 3.** The AS/MRFC acknowledges the BYE by replying with 200 OK back towards the transfer-from PSAP via IBCF#3.

**Step 4.** The IBCF#3 forwards the 200 OK to the transfer-from PSAP.

**Step 5.** The AS/MRFC sends a NOTIFY with subscription terminated indication to the transfer-from PSAP via IBCF#3.

**Step 6.** The IBCF#3 forwards the NOTIFY with subscription terminated indication to the transfer-from PSAP.

**Step 7.** The transfer-from PSAP sends a 200 OK towards the AS/MRFC via IBCF#3.

**Step 8.** The IBCF#3 forwards the 200 OK to the AS/MRFC.

**Step 9.** The AS/MRFC sends a NOTIFY via the IBCF#4 toward the transfer-to PSAP indicating the latest call state.

**Step 10.** The IBCF#4 forwards the NOTIFY to the transfer-to PSAP.

**Step 11.** The transfer-to PSAP replies back with a 200 OK.

**Step 12.** The IBCF#4 forwards the 200 OK to the AS/MRFC.

### 8.8.1.2.4.2 Transfer-to PSAP is a Legacy PSAP

This call flow illustrates a call flow scenario where the transfer-to PSAP is a legacy PSAP.

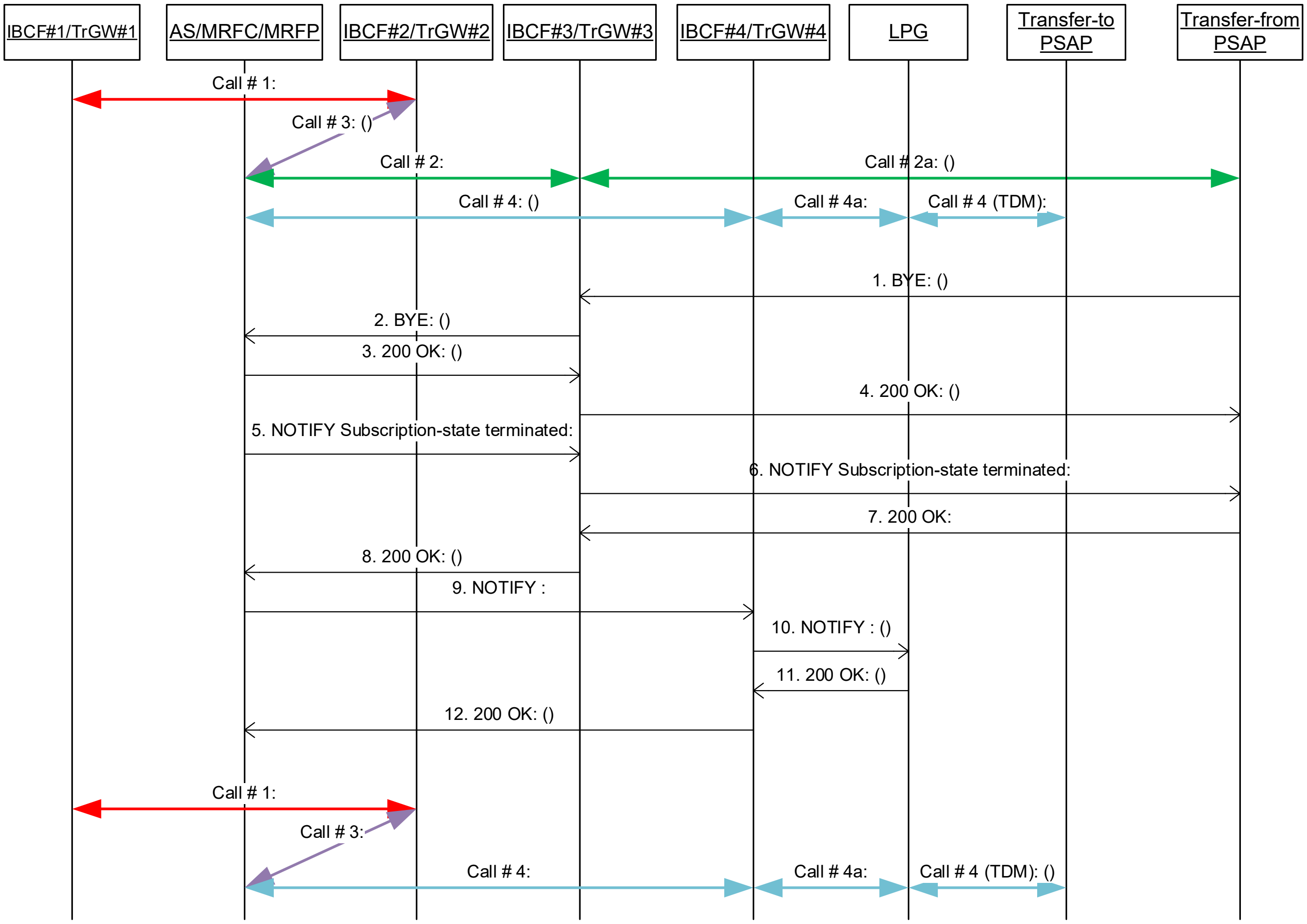


**Figure 8.34: Transfer-from i3 PSAP Drops out of Conference with Transfer-to Legacy PSAP**

**Step 1.** The transfer-from PSAP initiates a BYE towards the AS/MRFC to disconnect itself from the call via IBCF#3.

**Step 2.** The BYE is forwarded to the AS/MRFC by IBCF#3.

**Step 3.** The AS/MRFC acknowledges the BYE by replying with 200 OK back towards the transfer-from PSAP via IBCF#3.

**Step 4.** The IBCF#3 forwards the 200 OK to the transfer-from PSAP.

**Step 5.** The AS/MRFC sends a NOTIFY with subscription terminated indication to the transfer-from PSAP via IBCF#3.

**Step 6.** The IBCF#3 forwards the NOTIFY with subscription terminated indication to the transfer-from PSAP.

**Step 7.** The transfer-from PSAP sends a 200 OK towards the AS/MRFC via IBCF#3.

**Step 8.** The IBCF#3 forwards the 200 OK to the AS/MRFC.

**Step 9.** The AS/MRFC sends a NOTIFY to the LPG via IBCF#4 indicating the latest state of the call.

**Step 10.** The IBCF#4 forwards the NOTIFY to the LPG.

**Step 11.** The LPG replies back with a 200 OK to the AS/MRFC via IBCF#4.

**Step 12.** The IBCF#4 forwards the 200 OK to the AS/MRFC.

### 8.8.1.2.5 Transfer-to PSAP Completes the Transfer from the Conference

Since it is a two-party call between the calling party and the transfer-to PSAP, there is no reason to retain the conference bridge. The transfer-to PSAP initiates the release of AS/MRFC from the call. The transfer-to PSAP sets up a direct connection with the calling party through Call #5 at IBCF#2.

#### 8.8.1.2.5.1 Transfer-to PSAP is an i3 PSAP

This call flow illustrates the release of AS/MRFC from the conference by the transfer-to i3 PSAP.

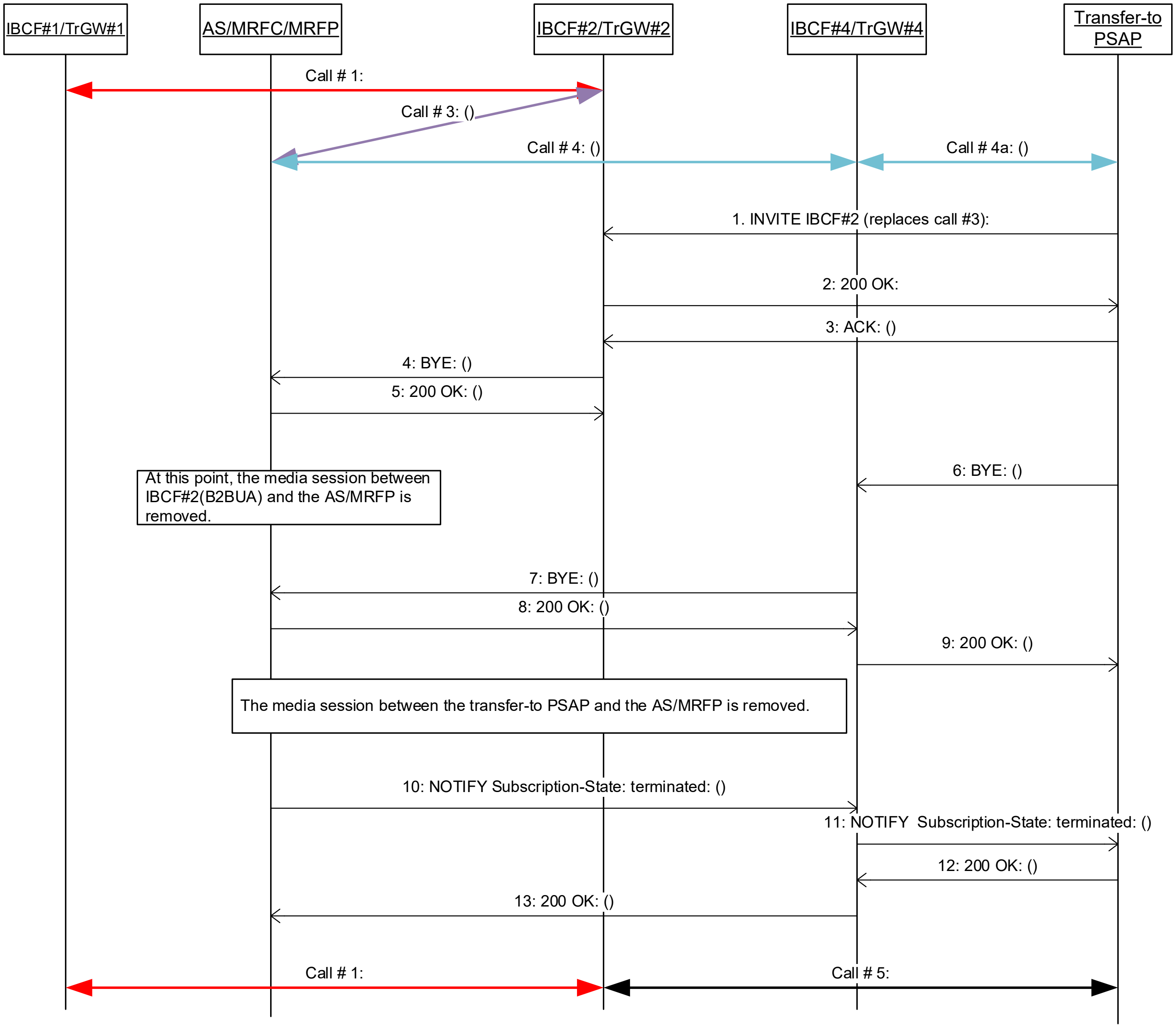

IBCF#1/TrGW#1
AS/MRFC/MRFP
IBCF#2/TrGW#2
IBCF#4/TrGW#4
Transfer-to PSAP
Call # 1:
Call # 3: ()
Call # 4: ()
Call # 4a: ()
1. INVITE IBCF#2 (replaces call #3):
2: 200 OK:
3: ACK: ()
4: BYE: ()
5: 200 OK: ()
6: BYE: ()
At this point, the media session between IBCF#2(B2BUA) and the AS/MRFP is removed.
7: BYE: ()
8: 200 OK: ()
9: 200 OK: ()
The media session between the transfer-to PSAP and the AS/MRFP is removed.
10: NOTIFY Subscription-State: terminated: ()
11: NOTIFY Subscription-State: terminated: ()
12: 200 OK: ()
13: 200 OK: ()
Call # 1:
Call # 5:

**Figure 8.35: Conference AS/MRFC Released by Transfer-to i3 PSAP**

**Step 1.** The transfer-to PSAP initiates an INVITE towards IBCF#2 to replace call #3 with a direct connection of the transfer-to PSAP via call #5.

**Step 2.** The IBCF#2 sends a 200 OK back to the transfer-to PSAP.

**Step 3.** The transfer-to PSAP sends an ACK in response to the 200 OK back to the IBCF#2.

**Step 4.** The IBCF#2 sends a BYE to the AS/MRFC to remove the media between IBCF#2 and the AS/MRFC.

**Step 5.** The AS/MRFC sends a 200 OK back to the IBCF#2. At this point the media between IBCF#2 and AS/MRFC is switched between IBCF#2 and the transfer-to PSAP represented by call #5.

**Step 6.** The transfer-to PSAP initiates the release of AS/MRFC from the call by sending a BYE via IBCF#4.

**Step 7.** The IBCF#4 forwards the BYE to the AS/MRFC.

**Step 8.** The AS/MRFC sends a 200 OK in response towards the transfer-to PSAP.

**Step 9.** The IBCF#4 forwards the 200 OK to the transfer-to PSAP. At this point the media session between transfer-to PSAP and AS/MRFC is switched between the IBCF#2 and the transfer-to PSAP represented by call #5.

**Step 10.** The AS/MRFC sends a NOTIFY with subscription state terminated indication towards the transfer-to PSAP via IBCF#4.

**Step 11.** The IBCF#4 forwards the NOTIFY with subscription state terminated indication to the transfer-to PSAP.

**Step 12.** The transfer-to PSAP sends the 200 OK to the AS/MRFC via IBCF#4.

**Step 13.** The IBCF#4 forwards the 200 OK to the AS/MRFC.

*At this point AS/MRFC is no longer involved with the conference. The original call (call #1) is directly connected to the transfer-to PSAP at IBCF#2/TrGW#2.*

### 8.8.1.2.5.2 Transfer-to PSAP is a Legacy PSAP

This call flow illustrates the release of AS/MRFC from the conference by the transfer-to legacy PSAP.

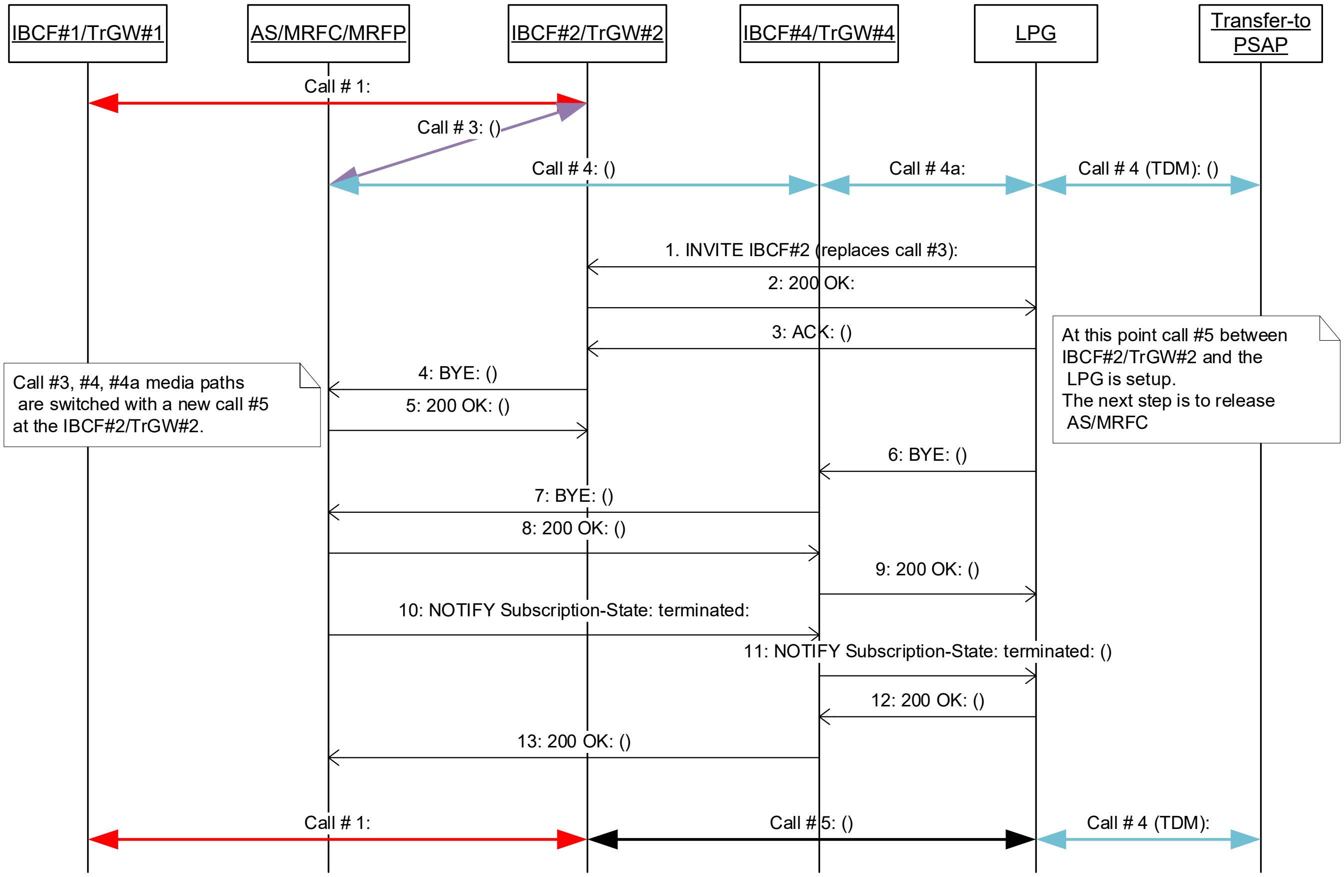

IBCF#1/TrGW#1
AS/MRFC/MRFP
IBCF#2/TrGW#2
IBCF#4/TrGW#4
LPG
Transfer-to PSAP
Call # 1:
Call # 3: ()
Call # 4: ()
Call # 4a:
Call # 4 (TDM): ()
1. INVITE IBCF#2 (replaces call #3):
2: 200 OK:
3: ACK: ()
4: BYE: ()
5: 200 OK: ()
6: BYE: ()
7: BYE: ()
8: 200 OK: ()
9: 200 OK: ()
10: NOTIFY Subscription-State: terminated:
11: NOTIFY Subscription-State: terminated: ()
12: 200 OK: ()
13: 200 OK: ()
Call # 1:
Call # 5: ()
Call # 4 (TDM):
Call #3, #4, #4a media paths are switched with a new call #5 at the IBCF#2/TrGW#2.
At this point call #5 between IBCF#2/TrGW#2 and the LPG is setup. The next step is to release AS/MRFC

**Figure 8.36: Conference AS/MRFC Released by Transfer-to Legacy PSAP**

**Step 1.** The LPG initiates an INVITE towards IBCF#2 to replace call #3 with a direct connection of the original call #1 with the transfer-to PSAP via LPG through call #5.

**Step 2.** The IBCF#2 sends a 200 OK back to the LPG.

**Step 3.** The LPG sends an ACK in response to the 200 OK back to the IBCF#2.

**Step 4.** The IBCF#2 sends a BYE to the AS/MRFC to remove the media between IBCF#2 and the AS/MRFC to remove call #3.

**Step 5.** The AS/MRFC sends a 200 OK back to the IBCF#2. At this point the media between IBCF#2 and AS/MRFC is switched.

**Step 6.** The LPG initiates the release of AS/MRFC from the call by sending a BYE to the AS/MRFC via IBCF#4.

**Step 7.** The IBCF#4 forwards the BYE to the AS/MRFC.

**Step 8.** The AS/MRFC sends a 200 OK in response towards the LPG via IBCF#4.

**Step 9.** The IBCF#4 forwards the 200 OK to the LPG. At this point the media session between transfer-to PSAP and AS/MRFC is switched.

**Step 10.** The AS/MRFC sends a NOTIFY with subscription state terminated indication towards the LPG via IBCF#4.

**Step 11.** The IBCF#4 forwards the NOTIFY with subscription state terminated indication to the LPG.

**Step 12.** The LPG sends the 200 OK to the AS/MRFC via IBCF#4.

**Step 13.** The IBCF#4 forwards the 200 OK to the AS/MRFC.

*At this point AS/MRFC is no longer involved with the conference. The original call (call #1) is directly connected to the transfer-to PSAP at IBCF#2/TrGW#2. The TDM call #4 between the LPG and the transfer-to Legacy PSAP stays intact.*

### 8.8.2 Support for Attended Emergency Call Transfer Requests from Legacy PSAPs to Transfer-to PSAPs/Destinations

Like attended transfers initiated by i3 PSAPs, when a legacy PSAP initiates an attended transfer, it must first create a conference on a bridge. As described in Clause 8.8.1, this bridge supports multimedia (voice, video, text) and resides in a conferencing AS. Media control for the conference is provided by an MRFC and media mixing is provided by an MRFP in the IMS-based NG9-1-1 Emergency Services Network.

The following subclauses describe flows associated with a transfer that is initiated by a legacy PSAP:

- Clause 8.8.2.1 covers the transfer-from legacy PSAP call scenario when media anchoring is done at the originating network-facing IBCF.
- Clause 8.8.2.2 covers the transfer-from legacy PSAP call scenario when media anchoring is done at the PSAP-facing IBCF.

#### 8.8.2.1 Media Anchoring at Originating Network-Facing IBCF Conditional on Supported Header

This clause describes a scenario where a legacy PSAP initiates the transfer of an emergency call. This scenario assumes that the calling device does not support the Replaces header, and the INVITE method with the Replaces header generated by the conferencing AS will be directed to an originating network-facing IBCF operating as a B2BUA rather than to the calling device.

#### 8.8.2.1.1 Conference Establishment

The flow depicted in Figure 8-35 illustrates the mechanism by which a legacy PSAP creates a conference at a conferencing AS. This call flow assumes that upon receiving an emergency session request, the originating network-facing IBCF will determine whether or not the incoming SIP INVITE message includes a Supported header containing the Replaces option-tag. If it does not, the IBCF will act as a B2BUA and include a Supported header containing the Replaces option-tag in the outgoing SIP INVITE message that it sends to the I-CSCF. Normal call processing will be applied to the emergency call as it progresses through the IMS-based NG9-1-1 Emergency Services Network and is delivered to the legacy PSAP via a PSAP-facing IBCF (not shown) that is operating as a proxy (or as a B2BUA that does not modify received headers, as described in RFC 7092 [Ref 33]), and a Legacy PSAP Gateway. In this example, the legacy PSAP determines that the call must be transferred and initiates the transfer by sending Dual Tone Multi-Frequency (DTMF) signaling to the LPG. The LPG interprets the incoming DTMF signaling, and interacts with a conferencing AS/MRFC to create a conference to support the transfer of the emergency call. The call flow illustrated in Figure 8-35 assumes that the calling device does not support the Replaces header, and that all signaling to/from the conferencing AS/MRFC to establish the initial conference between the transfer-from PSAP and the conferencing AS/MRFC flows through the I-CSCF.

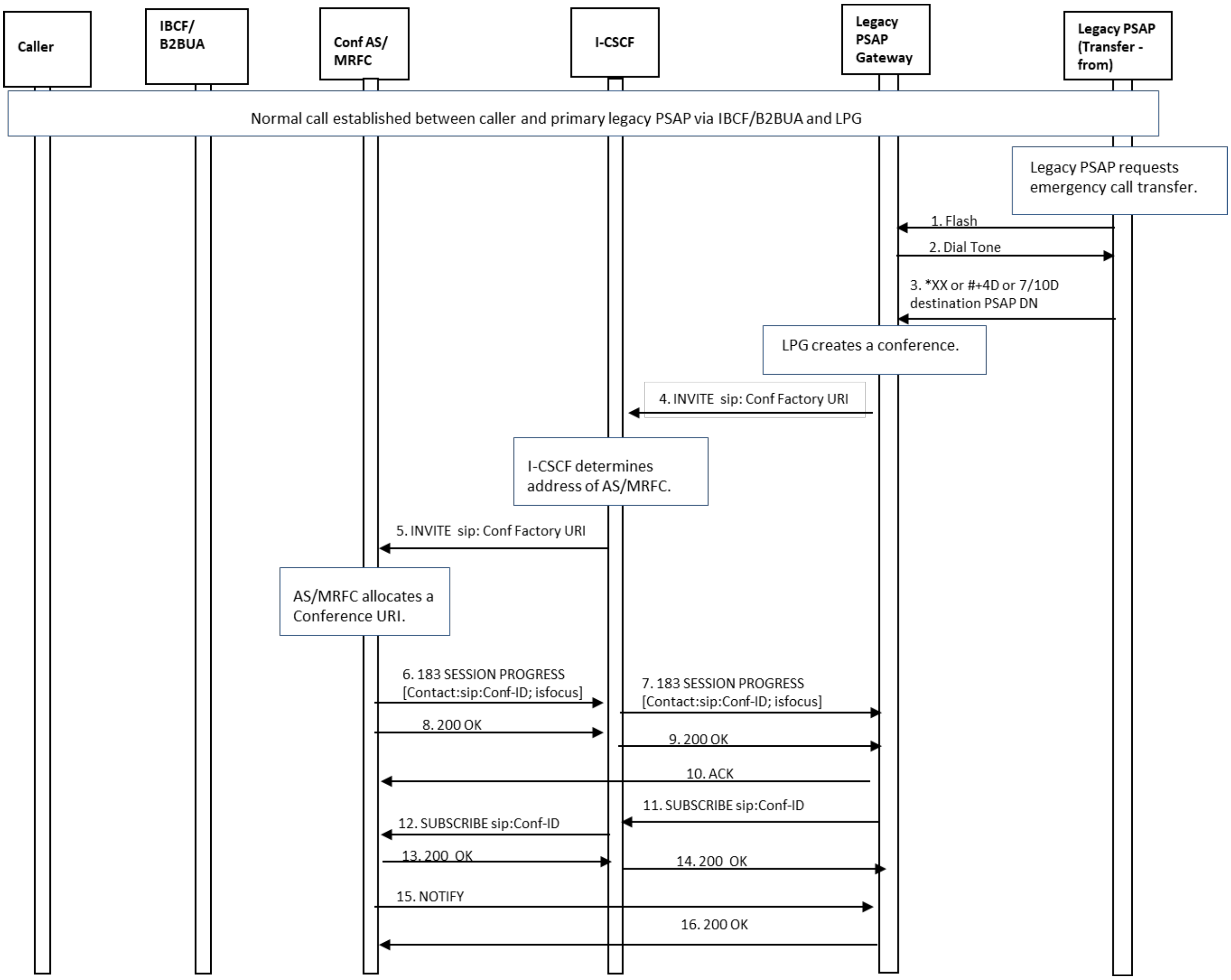

Caller
IBCF/ B2BUA
Conf AS/ MRFC
I-CSCF
Legacy PSAP Gateway
Legacy PSAP (Transfer - from)
Normal call established between caller and primary legacy PSAP via IBCF/B2BUA and LPG
Legacy PSAP requests emergency call transfer.
1. Flash
2. Dial Tone
3. *XX or #+4D or 7/10D destination PSAP DN
LPG creates a conference.
4. INVITE sip: Conf Factory URI
I-CSCF determines address of AS/MRFC.
5. INVITE sip: Conf Factory URI
AS/MRFC allocates a Conference URI.
6. 183 SESSION PROGRESS [Contact:sip:Conf-ID; isfocus]
7. 183 SESSION PROGRESS [Contact:sip:Conf-ID; isfocus]
8. 200 OK
9. 200 OK
10. ACK
11. SUBSCRIBE sip:Conf-ID
12. SUBSCRIBE sip:Conf-ID
13. 200 OK
14. 200 OK
15. NOTIFY
16. 200 OK

**Figure 8.37: Legacy PSAP Requests Transfer; LPG Establishes Conference with Conferencing AS/MRFC**

**Step 1.** Upon determining that an emergency call needs to be transferred, the legacy PSAP initiates a transfer request by sending a flash signal to the LPG.

**Step 2.** When the LPG receives the flash signal, it returns dial tone to the legacy PSAP and prepares to receive DTMF signaling.

**Step 3.** The legacy PSAP provides a *XX code, a string consisting of "# + 4-digits", or the 7/10-digit directory number associated with the transfer-to PSAP/destination.

**Step 4.** The LPG creates the conference by first sending an INVITE (via an IBCF [not shown]) to an I-CSCF in the IMS-based NG9-1-1 Emergency Services Network, using a conference factory URI that is known by/provisioned at the LPG. The SIP INVITE message includes a Resource Priority Header set to "esnet.1" to indicate that the session request is associated with the transfer of an emergency call.

*The I-CSCF resolves the conference factory URI and determines the address of the conferencing AS/MRFC.*

**Step 5.** The I-CSCF forwards the SIP INVITE message to the conferencing AS/MRFC.

*The conferencing AS/MRFC allocates a conference URI, based on local information, information gained from the conference-factory URI, and other information received in SIP signaling.*

**Step 6.** The conferencing AS/MRFC responds to the INVITE by returning a 183 SESSION PROGRESS message to the I-CSCF. The Contact header contains the conference URI for the conference allocated at the AS/MRFC and the isfocus feature parameter.

**Step 7.** The I-CSCF passes the 183 SESSION PROGRESS message (via an IBCF [not shown]) to the LPG.

**Step 8.** The conferencing AS/MRFC then returns a 200 OK message to the I-CSCF, to establish a session with the legacy PSAP via the LPG.

**Step 9.** The I-CSCF sends a 200 OK message (via an IBCF [not shown]) to the LPG.

**Step 10.** The LPG returns an ACK message to the conferencing AS/MRFC (via an IBCF [not shown]) in response to the 200 OK message.

*A session is established between the transfer-from legacy PSAP and the conferencing AS/MRFC. Note that the media session between the IBCF/B2BUA and the transfer-from legacy PSAP still exists at this time.*

**Step 11.** The LPG subscribes to the conference associated with the URI obtained from the Contact header provided by the conferencing AS/MRFC in the 180 SESSION PROGRESS message by sending a SIP SUBSCRIBE message containing the Conference ID via an IBCF (not shown) to the I-CSCF.

**Step 12.** The I-CSCF passes the SIP SUBSCRIBE message to the conferencing AS/MRFC.

**Step 13.** The conferencing AS/MRFC acknowledges the subscription request by sending a 200 OK message back to the I-CSCF.

**Step 14.** The I-CSCF passes the OK message to the LPG via an IBCF (not shown).

**Step 15.** The conferencing AS/MRFC then returns a NOTIFY message to the LPG via an IBCF (not shown) to provide subscription status information.

**Step 16.** The LPG responds by returning a 200 OK message via an IBCF (not shown) to the conferencing AS/MRFC.

#### 8.8.2.1.2 LPG Requests that the Conferencing AS Invite the IBCF/B2BUA to the Conference

After the LPG establishes the conference, it sends a REFER method to the conferencing AS/MRFC asking it to invite the IBCF/B2BUA to the conference. (As specified above, this flow assumes that the calling device does not support the Replaces header and that the transfer-from PSAP/LPG-facing IBCF [not shown] is operating as a proxy or as a B2BUA that does not modify received headers.) This portion of the emergency call transfer flow is the same as illustrated in Figure 8-20, with the LPG replacing the i3 PSAP.

#### 8.8.2.1.3 LPG Requests that the Conferencing AS Invite the Transfer-to PSAP to the Conference

Once the conferencing AS/MRFC has invited the IBCF/B2BUA to the conference, the LPG requests that the conferencing AS/MRFC invite the transfer-to PSAP to the conference by generating a REFER method following the procedures specified in RFC 7647 [Ref 34], with a Refer-To header that contains the URI of the transfer-to PSAP/agency, determined using one of the following methods. (See Clause 6.2.2.6 of NENA-STA-010.3 [Ref 27] for further details.)

- If the LPG receives a 7/10-digit destination number in the DTMF signaling from the legacy PSAP it will use this information to populate the URI in the Refer-To header of the outgoing REFER method.
- If the LPG receives a “# + 4-digits” via DTMF signaling from the legacy PSAP, it will add the appropriate NPA-NXX digits at the beginning of the 4-digit string, and use this information to populate the URI in the Refer-To header of the outgoing REFER method.
- If the LPG receives a code of the form “*XX” in the DTMF signaling from the legacy PSAP, it will do one of the following, based on trunk group provisioning:
    - The LPG will map the received “*XX” code to a static URI, and populate this URI in the Refer-To header of the outgoing REFER method.
    - The LPG will map the received “*XX” code to a service URN, and query an ECRF using this service URN and the location information received with the call. The LPG will then use the URI returned in the response from the ECRF to populate the Refer-To header of the outgoing REFER method.[26]

The procedures used by an LPG to request that the conferencing AS/MRFC invite the transfer-to PSAP to the conference follow the flows illustrated in Figure 8-21 and Figure 8-22, with the LPG replacing the transfer-from i3 PSAP in those flows. Note that the LPG will be responsible for creating the EIDO, populating whatever information it has available to it in the data structure (i.e., location information [by value or reference], as well as any Additional Data structures received with the call). If the LPG receives Additional Data “by value” with the call, the LPG will populate it in the EIDO by value. If the LPG receives Additional Data “by reference” with the call, it will populate it in the EIDO by reference. The LPG will include the EIDO by-reference in the SIP REFER method that it generates, following the procedures described in Clause 8.8.1.1.3.1. While the LPG does not know all of the information that the transfer-from PSAP may have acquired in its handling of the call, it is expected pass whatever information it has to the transfer-to PSAP, following the procedures described in Clause 8.8.1.1.3.1.

#### 8.8.2.1.4 Transfer-from Legacy PSAP Disconnects from the Conference

Once the transfer-from legacy PSAP determines that the transfer can be completed, the transfer-from legacy PSAP disconnects from the conference, as illustrated in Figure 8-36 and Figure 8-37.

##### 8.8.2.1.4.1 Transfer-to PSAP is an i3 PSAP

This call flow illustrates a scenario when the transfer-to PSAP is an i3 PSAP.

[26] This will require that the LPG be able to map all of the *XX codes supported by each PSAP that it serves to an appropriate service URN value that it can use to obtain the associated transfer-to destination address from the ECRF.

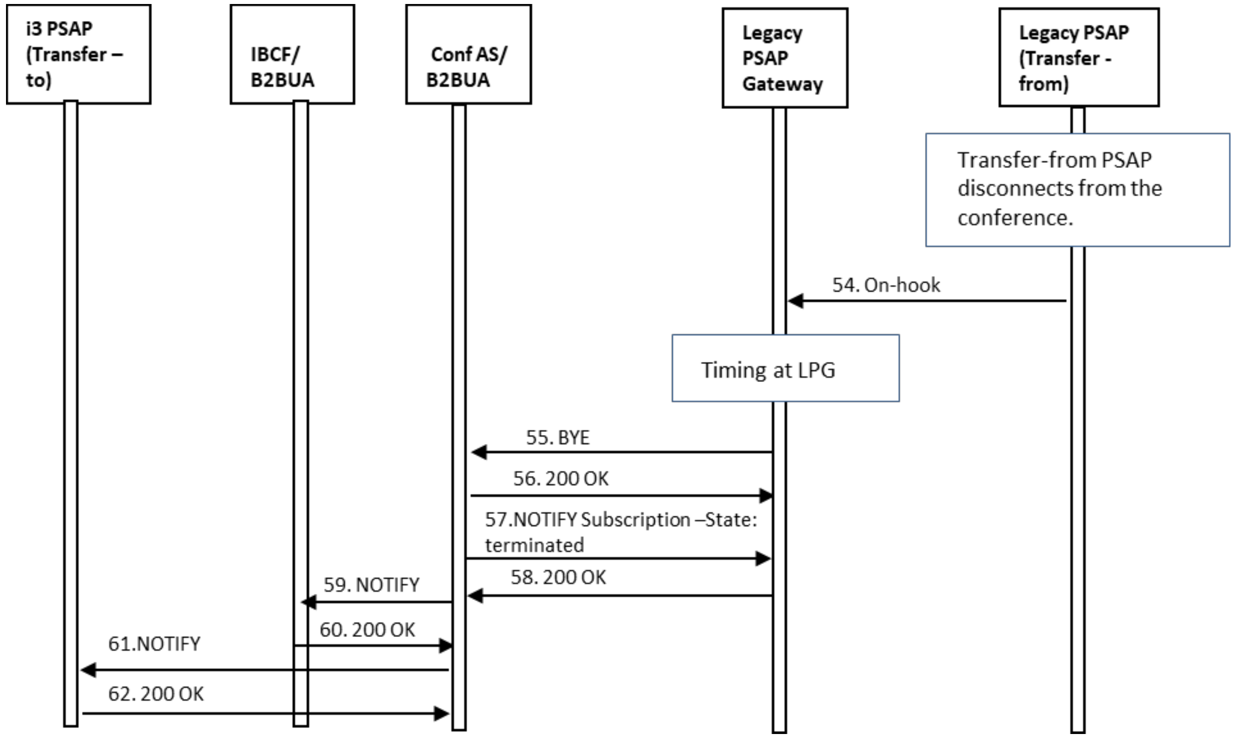


**Figure 8.38: Transfer-from Legacy PSAP Disconnects from the Conference – Transfer-to PSAP is an I3 PSAP**

**Step 54.** Upon determining that the emergency call transfer should be completed, the transfer-from legacy PSAP disconnects from the call by sending an on-hook signal to the LPG.

*The LPG sets a timer to distinguish a disconnect indication from a flash signal.*

**Step 55.** When the LPG determines that the legacy PSAP has disconnected, it sends a BYE message to the conferencing AS/MRFC (via the IBCF [not shown]).

**Step 56.** The conferencing AS/MRFC responds by returning a 200 OK message.

**Step 57.** The conferencing AS/MRFC then returns a NOTIFY message to the LPG (via the IBCF [not shown]) indicating that the subscription to the conference has been terminated.

**Step 58.** The LPG returns a 200 OK message in response to the NOTIFY message.

**Step 59.** The conferencing AS/MRFC then returns a NOTIFY message to the IBCF/B2BUA indicating that there has been a change to the subscription state.

**Step 60.** The IBCF/B2BUA returns a 200 OK message in response to the NOTIFY message.

**Step 61.** The conferencing AS/MRFC then returns a NOTIFY message to the transfer-to i3 PSAP (via the IBCF [not shown]) indicating that there has been a change to the subscription state.

**Step 62.** The transfer-to i3 PSAP returns a 200 OK message in response to the NOTIFY message.

### 8.8.2.1.4.2 Transfer-to PSAP is a Legacy PSAP

This call flow illustrates a scenario when the transfer-to PSAP is a legacy PSAP.

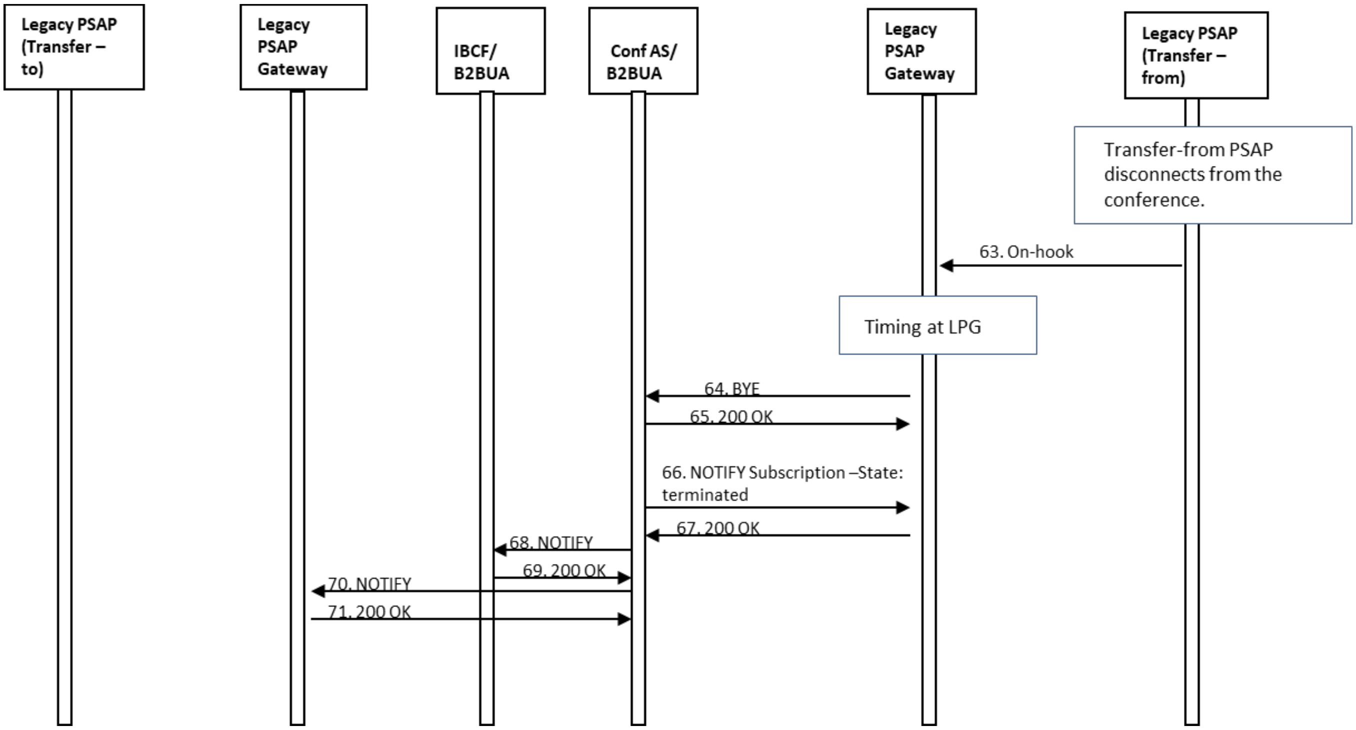


**Figure 8.39: Transfer-from Legacy PSAP Disconnects from the Conference – Transfer-to PSAP is a Legacy PSAP**

**Step 63.** Upon determining that the emergency call transfer should be completed, the transfer-from legacy PSAP disconnects from the call by sending an on-hook signal to the LPG.

*The LPG sets a timer to distinguish a disconnect indication from a flash signal.*

**Step 64.** When the LPG determines that the transfer-from PSAP has disconnected, it sends a BYE message to the conferencing AS/MRFC (via the IBCF [not shown]).

**Step 65.** The conferencing AS/MRFS responds by returning a 200 OK message.

**Step 66.** The conferencing AS/MRFC then returns a NOTIFY message to the LPG (via the IBCF [not shown]) indicating that the subscription to the conference has been terminated.

**Step 67.** The LPG returns a 200 OK message in response to the NOTIFY message.

**Step 68.** The conferencing AS/MRFC then returns a NOTIFY message to the IBCF/B2BUA indicating that there has been a change to the subscription state.

**Step 69.** The IBCF/B2BUA returns a 200 OK message in response to the NOTIFY message.

**Step 70.** The conferencing AS/MRFC then returns a NOTIFY message to the LPG that is serving the transfer-to PSAP (via the IBCF [not shown]) indicating that there has been a change to the subscription state.

**Step 71.** The LPG returns a 200 OK message in response to the NOTIFY message.

### 8.8.2.1.5 Transfer-to PSAP Completes the Transfer

The transfer-to PSAP then completes the transfer as illustrated in Figure 8-25 and Figure 8-26. As described in Clause 8.8.1.1.5.1, the connection between the caller and the IBCF/B2BUA is unaffected by the completion of the transfer by the transfer-to PSAP.

### 8.8.2.2 Media Anchoring at PSAP-Facing IBCF

This clause provides the call flows where the media anchoring is done at the PSAP-facing IBCF/Transition Gateway (TrGW). In these call flows the transfer-from PSAP is a legacy PSAP.

#### 8.8.2.2.1 Conference Establishment

The call flow below illustrates the mechanism by which a legacy PSAP creates a conference at the AS/MRFC. The scenario illustrated in this call flow is for media to be anchored at the PSAP-facing IBCF/B2BUA. The (transfer-from) legacy PSAP determines that the call must be transferred and initiates the transfer by sending DTMF signaling to the LPG. The LPG interprets the incoming DTMF signaling, and interacts with a conferencing AS/MRFC to create a conference to support the transfer of the emergency call.

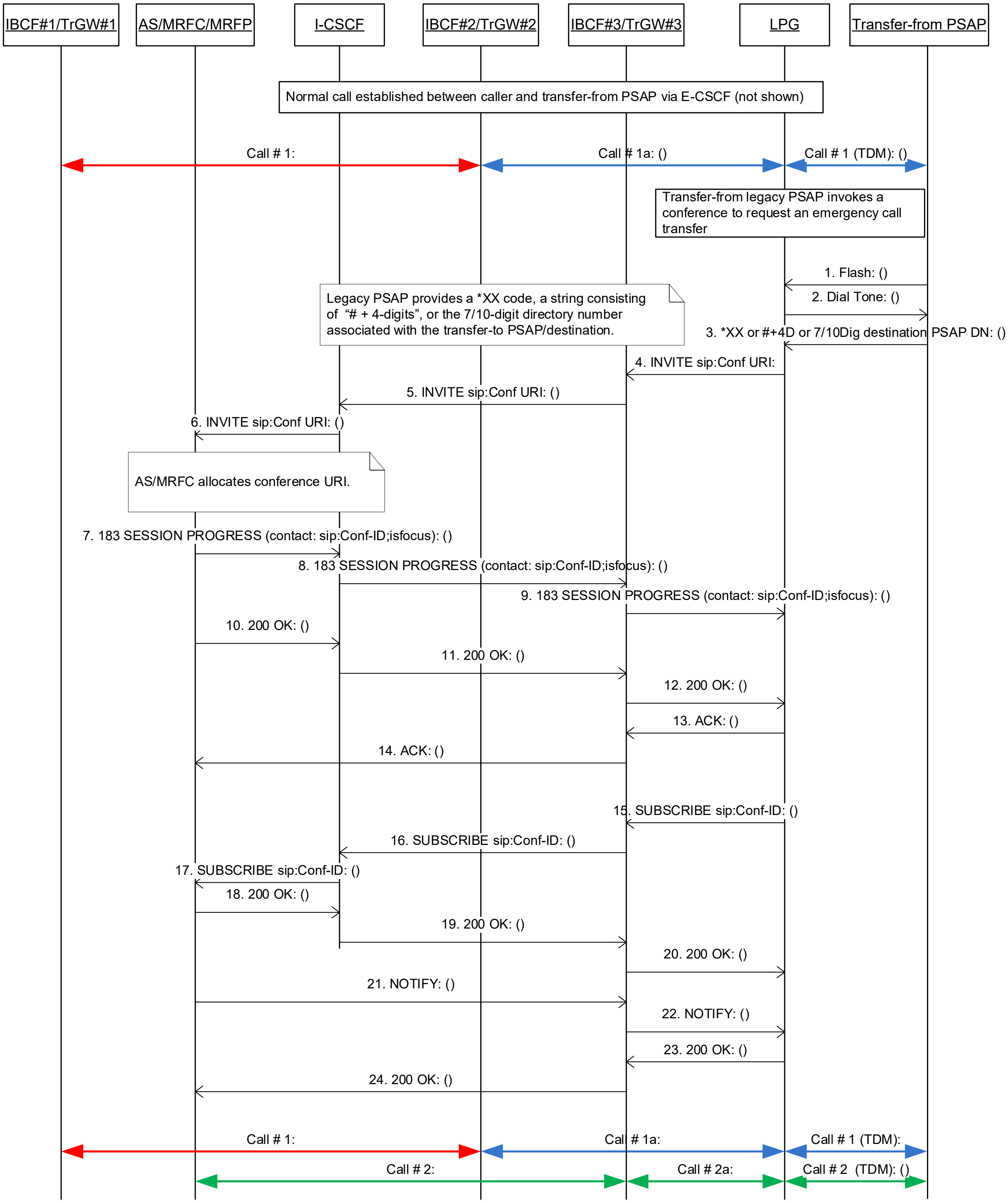

IBCF#1/TrGW#1
AS/MRFC/MRFP
I-CSCF
IBCF#2/TrGW#2
IBCF#3/TrGW#3
LPG
Transfer-from PSAP
Normal call established between caller and transfer-from PSAP via E-CSCF (not shown)
Call # 1:
Call # 1a: ()
Call # 1 (TDM): ()
Transfer-from legacy PSAP invokes a conference to request an emergency call transfer
1. Flash: ()
2. Dial Tone: ()
Legacy PSAP provides a *XX code, a string consisting of "# + 4-digits", or the 7/10-digit directory number associated with the transfer-to PSAP/destination.
3. *XX or #+4D or 7/10Dig destination PSAP DN: ()
4. INVITE sip:Conf URI:
5. INVITE sip:Conf URI: ()
6. INVITE sip:Conf URI: ()
AS/MRFC allocates conference URI.
7. 183 SESSION PROGRESS (contact: sip:Conf-ID;isfocus): ()
8. 183 SESSION PROGRESS (contact: sip:Conf-ID;isfocus): ()
9. 183 SESSION PROGRESS (contact: sip:Conf-ID;isfocus): ()
10. 200 OK: ()
11. 200 OK: ()
12. 200 OK: ()
13. ACK: ()
14. ACK: ()
15. SUBSCRIBE sip:Conf-ID: ()
16. SUBSCRIBE sip:Conf-ID: ()
17. SUBSCRIBE sip:Conf-ID: ()
18. 200 OK: ()
19. 200 OK: ()
20. 200 OK: ()
21. NOTIFY: ()
22. NOTIFY: ()
23. 200 OK: ()
24. 200 OK: ()
Call # 1:
Call # 1a:
Call # 1 (TDM):
Call # 2:
Call # 2a:
Call # 2 (TDM): ()

**Figure 8.40: Legacy PSAP Establishes Conference with Conferencing AS/MRFC**

**Step 1.** The transfer-from legacy PSAP decides to transfer the emergency call and initiates the transfer by sending a flash indication to the LPG.

**Step 2.** The LPG generates a dial tone signal in response back to the transfer-from legacy PSAP.

**Step 3.** The legacy PSAP provides a *XX code, a string consisting of "# + 4-digits", or the 7/10-digit directory number associated with the transfer-to PSAP/destination.

**Step 4.** The LPG creates the conference by first sending an INVITE towards the AS/MRFC via IBCF#3 using a conference factory URI that is known by/provisioned at the LPG. The SIP INVITE message includes a Resource Priority Header set to "esnet.1" to indicate that the session request is associated with the transfer of an emergency call.

**Step 5.** The IBCF#3 forwards the INVITE to the I-CSCF.

**Step 6.** The I-CSCF determines the address of the conferencing AS/MRFC and forwards the INVITE to the AS/MRFC.

NOTE: I-CSCF does not add itself to the Record-Route header.

**Step 7.** The conferencing AS/MRFC allocates a conference URI, based on local information, information gained from the conference-factory URI, and other information received in SIP signaling. The conferencing AS/MRFC responds to the INVITE by returning a 183 SESSION PROGRESS to the I-CSCF. The Contact header contains the conference URI for the conference allocated at the AS/MRFC and the "isfocus" feature parameter indicating a conference call.

**Step 8.** The I-CSCF forwards the 183 SESSION PROGRESS to the IBCF#3.

**Step 9.** The IBCF#3 forwards the 183 SESSION PROGRESS to the LPG.

**Step 10.** The AS/MRFC sends a 200 OK to the I-CSCF in response to the INVITE message.

**Step 11.** The I-CSCF forwards the 200 OK to the IBCF#3.

**Step 12.** The IBCF#3 forwards the 200 OK to the LPG.

**Step 13.** The LPG returns an ACK acknowledging the receipt of 200 OK to the IBCF#3.

**Step 14.** The IBCF#3 forwards the ACK to the AS/MRFC.

*At this point the media session is established between the MRFP and the transfer-from PSAP and denoted as call #2. However, the UE is still connected to the transfer-from PSAP as call #1.*

**Step 15.** The LPG sends a SUBSCRIBE to the AS/MRFC to stay informed regarding the status of conference call to the IBCF#3.

**Step 16.** The IBCF#3 forwards the SUBSCRIBE to the I-CSCF.

**Step 17.** The I-CSCF forwards the SUBSCRIBE to the AS/MRFC.

**Step 18.** The AS/MRFC sends a 200 OK back to the I-CSCF.

**Step 19.** The I-CSCF forwards the 200 OK to the IBCF#3.

**Step 20.** The IBCF#3 forwards the 200 OK to the LPG.

**Step 21.** The AS/MRFC sends a NOTIFY to the LPG via IBCF#3.

**Step 22.** The IBCF#3 forwards the NOTIFY to the LPG.

**Step 23.** The LPG sends a 200 OK back to the AS/MRFC in response to NOTIFY via IBCF#3.

**Step 24.** The IBCF#3 forwards the 200 OK to the AS/MRFC.

#### 8.8.2.2.2 LPG Requests that the Conferencing AS Bridge the Original Call at IBCF#2/B2BUA

Once a new media path is established between the LPG and the AS/MRFP, the LPG sends a REFER to the AS/MRFC requesting that it invite the IBCF#2/B2BUA to the conference. As a result, the AS/MRFC initiates an

INVITE toward the PSAP-facing IBCF#2/B2BUA to invite it to the conference. The intent of this call flow is to show a new media establishment between the AS/MRFP and the IBCF#2/B2BUA. This portion of the emergency call transfer flow is the same as illustrated in Clause 8.8.1.2.2 Figure 8-28: Application Server (AS) Bridges Call #1 and Call #2 via IBCF#2 with the LPG replacing the i3 PSAP.

### 8.8.2.2.3 LPG Requests that the Conferencing AS Invite the Transfer-to PSAP to the Conference

At this point the original call is connected through the conference. The LPG then requests the AS/MRFC to invite the transfer-to PSAP to the call using REFER per RFC 7647 [Ref 34]. The rules to generate the URI in the Refer-To field as described in Clause 8.8.2.1.3 will also apply in this clause.

For media anchoring at a PSAP-facing IBCF, the following scenarios apply: where the transfer-to PSAP is an i3 PSAP, Clause 8.8.1.2.3.1 Figure 8-29: Application Server (AS) Invites Transfer-to i3 PSAP to Conference applies; where the transfer-to PSAP is a legacy PSAP, Clause 8.8.1.2.3.2 Figure 8-30: Application Server (AS) Invites Transfer-to Legacy PSAP to Conference applies. The only difference in the call flows in Clause 8.8.1.2.3.1 and Clause 8.8.1.2.3.2 is that since the transfer-from PSAP is a legacy PSAP, the LPG replaces the i3 PSAP in the flow. The rules to generate the EIDO either by-reference or by-value are same as described in Clause 8.8.2.1.3.

### 8.8.2.2.4 Transfer-from Legacy PSAP Disconnects from the Conference

Upon a successful conference establishment between the caller and the transfer-to PSAP, the transfer-to PSAP can take over the handling of the call. The transfer-from PSAP determines that the transfer can be completed and drops from the conference. This call flow illustrates the release of transfer-from PSAP from the call path during an emergency call transfer.

#### 8.8.2.2.4.1 Transfer-to PSAP is an i3 PSAP

This call flow illustrates the disconnection of the transfer-from legacy PSAP from the conference when the transfer-to PSAP is an i3 PSAP.

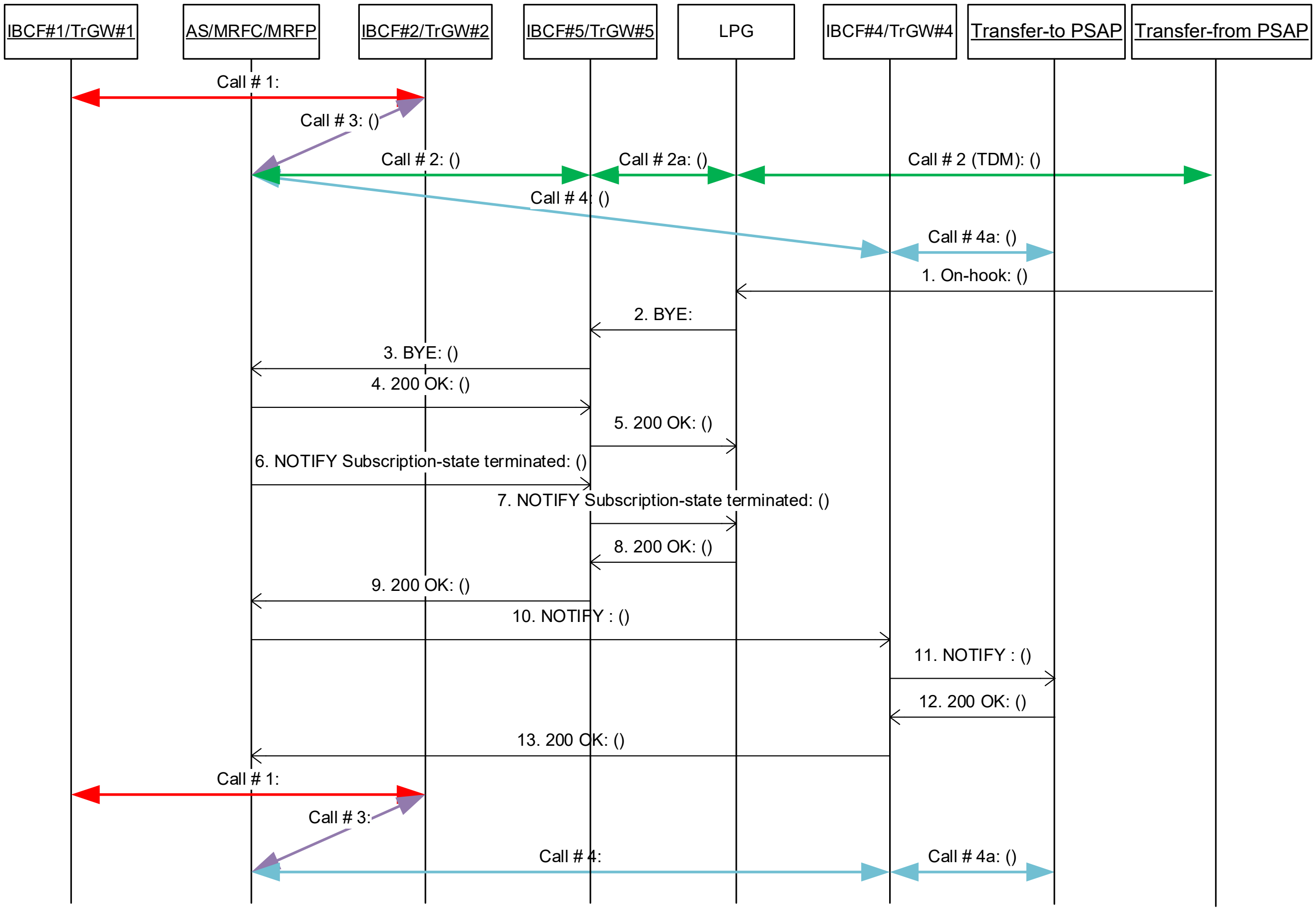


**Figure 8.41: Transfer-from Legacy PSAP Drops out of Conference with Transfer-to i3 PSAP**

**Step 1.** The transfer-from PSAP initiates its disconnect from the conference by sending an “On-hook” indication to the LPG.

**Step 2.** The LPG generates a BYE towards the AS/MRFC to disconnect itself from the call via IBCF#5.

**Step 3.** The BYE is forwarded to the AS/MRFC by IBCF#5.

**Step 4.** The AS/MRFC acknowledges the BYE by replying with 200 OK back to the IBCF#5.

**Step 5.** The IBCF#5 forwards the 200 OK to the LPG.

**Step 6.** The AS/MRFC sends a NOTIFY with subscription terminated indication to the LPG via IBCF#5.

**Step 7.** The IBCF#5 forwards the NOTIFY with subscription terminated indication to the LPG.

**Step 8.** The LPG sends a 200 OK toward the AS/MRFC via IBCF#5.

**Step 9.** The IBCF#5 forwards the 200 OK to the AS/MRFC.

**Step 10.** The AS/MRFC sends a NOTIFY to the transfer-to PSAP via IBCF#4 indicating the latest call state.

**Step 11.** The IBCF#4 forwards the NOTIFY to the transfer-to PSAP.

**Step 12.** The transfer-to PSAP replies back with a 200 OK to the IBCF#4.

**Step 13.** The IBCF#4 forwards the 200 OK to the AS/MRFC.

### 8.8.2.2.4.2 Transfer-to PSAP is a Legacy PSAP

This call flow illustrates the disconnection of the transfer-from legacy PSAP from the conference when the transfer-to PSAP is also a legacy PSAP.

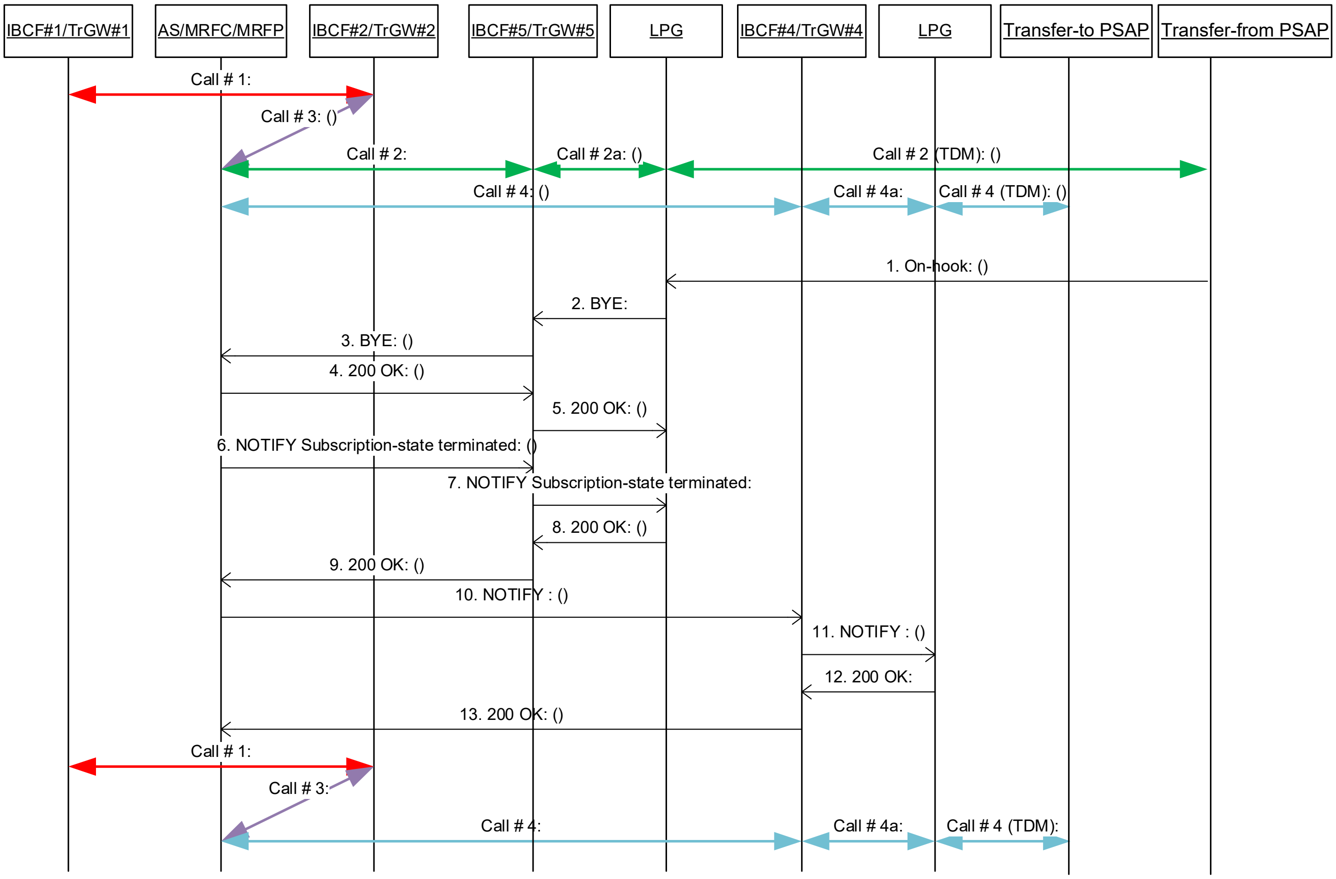


**Figure 8.42: Transfer-from Legacy PSAP Drops out of Conference with Transfer-to Legacy PSAP**

**Step 1.** The transfer-from PSAP initiates its disconnect from the conference by sending an “On-hook” indication to the LPG.

**Step 2.** The LPG generates a BYE towards the AS/MRFC to disconnect itself from the call via IBCF#5.

**Step 3.** The BYE is forwarded to the AS/MRFC by the IBCF#5.

**Step 4.** The AS/MRFC acknowledges the BYE by replying with 200 OK back to the IBCF#5.

**Step 5.** The IBCF#5 forwards the 200 OK to the LPG.

**Step 6.** The AS/MRFC sends a NOTIFY with subscription terminated indication to the LPG via IBCF#5.

**Step 7.** The IBCF#5 forwards the NOTIFY with subscription terminated indication to the LPG.

**Step 8.** The LPG sends a 200 OK towards the AS/MRFC via IBCF#5.

**Step 9.** The IBCF#5 forwards the 200 OK to the AS/MRFC.

**Step 10.** The AS/MRFC sends a NOTIFY to the LPG via IBCF#4 indicating the latest call state.

**Step 11.** The IBCF#4 forwards the NOTIFY to the LPG.

**Step 12.** The LPG replies back with a 200 OK to the IBCF#4.

**Step 13.** The IBCF#4 forwards the 200 OK to the AS/MRFC.

#### 8.8.2.2.5 Transfer-to PSAP Completes the Transfer

Since the transfer-from legacy PSAP is no longer part of the call, the call flow procedure to release the AS/MRFC and complete the transfer in this step is same as described in Clause 8.8.2.1.5. There are two possible scenarios to consider here.

In the first scenario, the transfer-to i3 PSAP releases the AS/MRFC and completes the transfer. The call flow for this scenario is same as described in Clause 8.8.1.2.5.1.

The second scenario is when the transfer-to legacy PSAP releases the AS/MRFC and completes the transfer. The call flow for this scenario is same as described in Clause 8.8.1.2.5.2.

## 8.8.3 Support for Blind Transfer Requests from i3 PSAPs to Transfer-to PSAPs/Destinations

The blind transfer procedures described in this clause are based on 3GPP TS 24.629 [Ref 49]. The Explicit Communication Transfer (ECT) mechanism specified in 3GPP TS 24.629 [Ref 49] assumes the presence of an ECT AS (rather than the Conferencing AS present in architectures that support attended transfer). The ECT AS is responsible for receiving a REFER method from a transfer-from PSAP (via an I-CSCF in the context of an IMS-based NG9-1-1 Emergency Services Network), storing the value of the Refer-To header field (which it will use later to correlate the new communication with this REFER dialog), optionally storing the value of the Referred-By header field (if it wants to ensure that the Referred-By is correct on the resulting INVITE request), and forwarding the request to the caller according to basic communication procedures specified 3GPP TS 24.229 [Ref 2].

Note that blind transfers initiated by legacy PSAPs use the same procedures as attended transfers, except that the transfer-from PSAP disconnects any time after the transfer-to destination acknowledges the incoming call.

### 8.8.3.1 Blind Transfer from i3 PSAP to i3 PSAP

This call flow assumes that normal call processing will be applied to the emergency call as it progresses through the IMS-based NG9-1-1 Emergency Services Network and is delivered to an i3 PSAP. In this example, the (transfer-from) i3 PSAP determines that the call must be transferred and initiates a blind transfer of the emergency call to another (transfer-to) i3 PSAP. The i3 PSAP determines the URI associated with the transfer-to PSAP by querying an ECRF using a service URN in the “urn:emergency:service:responder” family and the location information received with the call (not shown in figure below). The i3 PSAP then uses the URI returned in the response from the ECRF to populate the Refer-To header of the outgoing REFER method. This call flow assumes that the REFER sent by the transfer-from PSAP to the ECT AS to support the blind transfer flows through the I-CSCF.

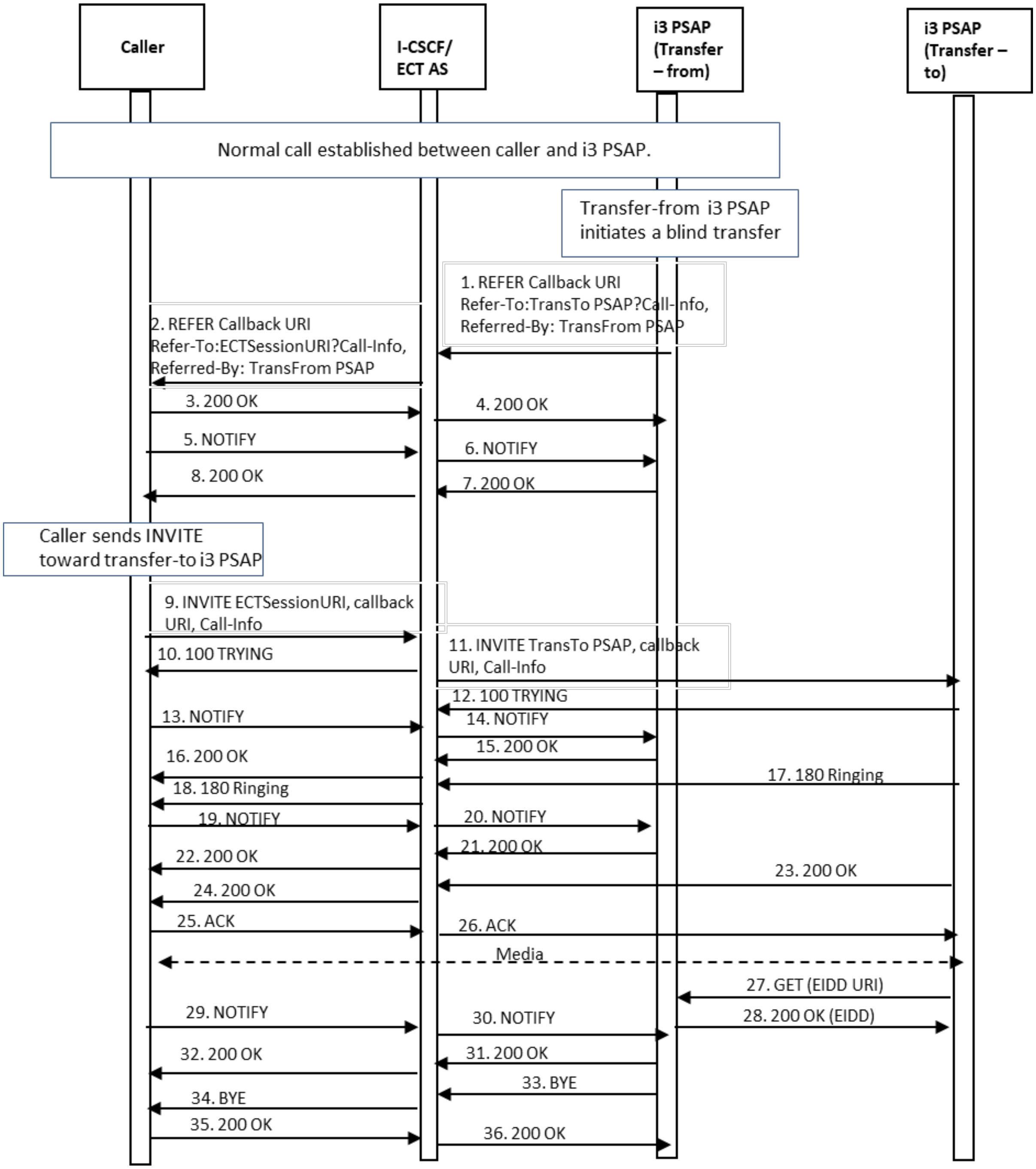

Caller
I-CSCF/ ECT AS
i3 PSAP (Transfer – from)
i3 PSAP (Transfer – to)
Normal call established between caller and i3 PSAP.
Transfer-from i3 PSAP initiates a blind transfer
1. REFER Callback URI Refer-To:TransTo PSAP?Call-Info, Referred-By: TransFrom PSAP
2. REFER Callback URI Refer-To:ECTSessionURI?Call-Info, Referred-By: TransFrom PSAP
3. 200 OK
4. 200 OK
5. NOTIFY
6. NOTIFY
8. 200 OK
7. 200 OK
Caller sends INVITE toward transfer-to i3 PSAP
9. INVITE ECTSessionURI, callback URI, Call-Info
10. 100 TRYING
11. INVITE TransTo PSAP, callback URI, Call-Info
12. 100 TRYING
13. NOTIFY
14. NOTIFY
15. 200 OK
16. 200 OK
17. 180 Ringing
18. 180 Ringing
19. NOTIFY
20. NOTIFY
21. 200 OK
22. 200 OK
23. 200 OK
24. 200 OK
25. ACK
26. ACK
Media
27. GET (EIDD URI)
29. NOTIFY
30. NOTIFY
28. 200 OK (EIDD)
32. 200 OK
31. 200 OK
33. BYE
34. BYE
35. 200 OK
36. 200 OK

**Figure 8.43: Blind Transfer: Transfer-from i3 PSAP to Transfer-to i3 PSAP**

**Step 1.** The transfer-from PSAP determines that it needs to transfer an emergency call. It sends a REFER via the I-CSCF to the ECT AS with a To header field set to the callback URI associated with the emergency caller, a Refer-To header field set to the transfer-to i3 PSAP URI, a Referred-By header field set to the transfer-from i3 PSAP URI, and an escaped Call-Info header containing a reference URI that points to the EIDO data structure and a purpose parameter of "eido". The REFER request is sent in the existing dialog between the caller and the transfer-from i3 PSAP.

After determining that the transfer-from PSAP is allowed to transfer calls, the ECT AS generates an ECT session identifier URI, addressed to itself, and replaces the Refer-To header field value with the ECT session identifier URI. This ensures that the ECT AS will remain in the path.

**Step 2.** The ECT AS forwards the REFER to the caller's UE via IBCFs at the edge of the Emergency Services Network and at the edge of the originating network (not shown).

**Step 3.** The caller's UE accepts the REFER request and returns a 200 OK to the ECT AS via IBCFs at the edge of the Emergency Services Network and at the edge of the originating network (not shown).

**Step 4.** The ECT AS forwards the 200 OK via an IBCF (not shown) toward the transfer-from PSAP.

**Step 5.** The caller's UE sends a NOTIFY toward the ECT AS via IBCFs (not shown).

**Step 6.** The ECT AS sends a NOTIFY towards the transfer-from PSAP via an IBCF (not shown).

**Step 7.** The transfer-from PSAP sends a 200 OK back to the ECT AS via an IBCF (not shown).

**Step 8.** The ECT AS forwards the 200 OK to the caller's UE via IBCFs (not shown).

**Step 9.** The caller's UE initiates a call establishment toward the transfer-to i3 PSAP by sending a SIP INVITE message via the I-CSCF to the ECT AS. The INVITE message includes the ECT AS URI, the callback URI, and the Call-Info header received in the REFER.

**Step 10.** The ECT AS returns a 100 TRYING message to the caller's UE.

**Step 11.** The ECT AS forwards the INVITE via an IBCF (not shown) toward the transfer-to i3 PSAP.

**Step 12.** The transfer-to i3 PSAP returns a 100 TRYING message to the ECT AS.

**Step 13.** The caller's UE sends a NOTIFY message to the ECT AS to report the progress of the REFER request.

**Step 14.** The ECT AS sends a NOTIFY message to the transfer-from i3 PSAP to report the progress of the REFER request.

**Step 15.** The transfer-from i3 PSAP returns a 200 OK to the ECT AS in response to the NOTIFY message.

**Step 16.** The ECT AS returns a 200 OK message to the caller's UE.

**Step 17.** The transfer-to i3 PSAP generates a 180 RINGING message and sends it to the ECT AS via an IBCF (not shown).

**Step 18.** The ECT AS forwards the 180 RINGING message to the caller's UE.

**Step 19.** The caller's UE sends a NOTIFY message to the ECT AS to report the progress of the REFER request.

**Step 20.** The ECT AS sends a NOTIFY message to the transfer-from i3 PSAP to report the progress of the REFER request.

**Step 21.** The transfer-from i3 PSAP returns a 200 OK to the ECT AS in response to the NOTIFY message.

**Step 22.** The ECT AS returns a 200 OK message to the caller's UE.

**Step 23.** The transfer-to i3 PSAP sends a 200 OK message to the ECT AS (via IBCFs that are not shown) in response to previously received SIP INVITE message indicating that it has answered the call.

**Step 24.** The ECT AS sends a 200 OK message to the caller UE (via IBCFs that are not shown) in response to the previously received SIP INVITE message indicating that the transfer-to PSAP has answered the call.

**Step 25.** The caller's UE responds to the 200 OK by returning an ACK to the ECT AS (via IBCFs that are not shown).

**Step 26.** The ECT AS sends an ACK to the transfer-to i3 PSAP (via an IBCF that is not shown) in response to the 200 OK.

*Media is now flowing between the caller's UE and the transfer-to i3 PSAP*.

**Step 27.** The transfer-to i3 PSAP queries the transfer-from i3 PSAP for the EIDO by including the URI provided in the Call-Info header in an outgoing GET request.

**Step 28.** The transfer-from PSAP returns the EIDO to the transfer-to i3 PSAP in a 200 OK.

**Step 29.** The caller's UE sends a NOTIFY message to the ECT AS to report the progress of the REFER request.

**Step 30.** The ECT AS sends a NOTIFY message to the transfer-from i3 PSAP to report the progress of the REFER request.

**Step 31.** The transfer-from i3 PSAP returns a 200 OK to the ECT AS in response to the NOTIFY message.

**Step 32.** The ECT AS returns a 200 OK message to the caller's UE.

**Step 33.** Once the transfer-from i3 PSAP has determined that the call between the caller and the transfer-to i3 PSAP is active, it sends a BYE message to the ECT AS, terminating the original emergency dialog.

**Note:** Unlike the procedures defined in 3GPP TS 24.629 [Ref 49], which specify that a BYE will be sent by the transfer-from party after the REFER request has been accepted, the transfer-from PSAP must wait until it receives a notification that a 200 OK has been returned by the transfer-to PSAP (see Step 30) before sending a BYE message to terminate the dialog with the caller. This is necessary in the context of emergency services to ensure that a connection to the caller is maintained even if the transfer is unsuccessful.

**Step 34.** The ECT AS passes the BYE message associated with the original emergency dialog to the caller's UE.

**Step 35.** The caller's UE responds by returning a 200 OK to the ECT AS.

**Step 36.** The ECT AS returns a 200 OK to the transfer-from PSAP.

*Media between the caller and the transfer-from PSAP is terminated.*

### 8.8.3.2 Blind Transfer from i3 PSAP to Legacy PSAP

This call flow assumes that normal call processing will be applied to the emergency call as it progresses through the IMS-based NG9-1-1 Emergency Services Network and is delivered via an LPG to a legacy PSAP. In this example, the (transfer-from) i3 PSAP determines that the call must be transferred and initiates a blind transfer of the emergency call to a transfer-to legacy PSAP. The i3 PSAP determines the URI associated with the transfer-to PSAP by querying an ECRF using a service URN in the "urn:emergency:service:responder" family and the location information received with the call (not shown in figure below). The i3 PSAP then uses the URI returned in the response from the ECRF to populate the Refer-To header of the outgoing REFER method. This call flow assumes that the REFER sent by the transfer-from i3 PSAP to the ECT AS to support the blind transfer flows through the I-CSCF.

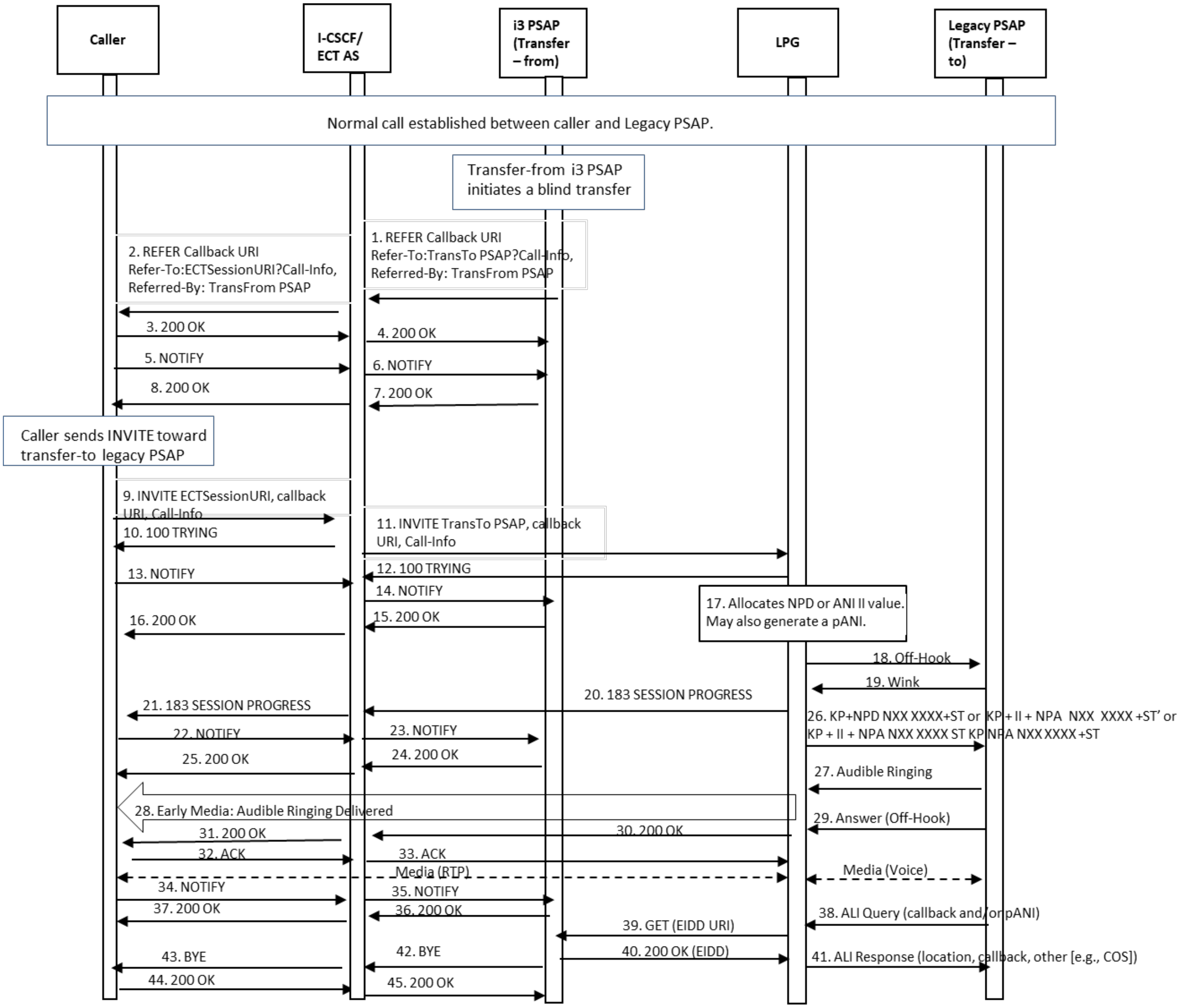

Caller
I-CSCF/ ECT AS
i3 PSAP (Transfer – from)
LPG
Legacy PSAP (Transfer – to)
Normal call established between caller and Legacy PSAP.
Transfer-from i3 PSAP initiates a blind transfer
1. REFER Callback URI Refer-To:TransTo PSAP?Call-Info, Referred-By: TransFrom PSAP
2. REFER Callback URI Refer-To:ECTSessionURI?Call-Info, Referred-By: TransFrom PSAP
3. 200 OK
4. 200 OK
5. NOTIFY
6. NOTIFY
8. 200 OK
7. 200 OK
Caller sends INVITE toward transfer-to legacy PSAP
9. INVITE ECTSessionURI, callback URI, Call-Info
10. 100 TRYING
11. INVITE TransTo PSAP, callback URI, Call-Info
12. 100 TRYING
13. NOTIFY
14. NOTIFY
16. 200 OK
15. 200 OK
17. Allocates NPD or ANI II value. May also generate a pANI.
18. Off-Hook
19. Wink
20. 183 SESSION PROGRESS
21. 183 SESSION PROGRESS
26. KP+NPD NXX XXXX+ST or KP + II + NPA NXX XXXX +ST' or KP + II + NPA NXX XXXX ST KP NPA NXX XXXX +ST
22. NOTIFY
23. NOTIFY
25. 200 OK
24. 200 OK
27. Audible Ringing
28. Early Media: Audible Ringing Delivered
29. Answer (Off-Hook)
31. 200 OK
30. 200 OK
32. ACK
33. ACK
Media (RTP)
Media (Voice)
34. NOTIFY
35. NOTIFY
37. 200 OK
36. 200 OK
38. ALI Query (callback and/or pANI)
39. GET (EIDD URI)
40. 200 OK (EIDD)
43. BYE
42. BYE
41. ALI Response (location, callback, other [e.g., COS])
44. 200 OK
45. 200 OK

**Figure 8-42: Blind Transfer: Transfer-from i3 PSAP to Transfer-to Legacy PSAP**

**Step 1.** The transfer-from PSAP determines that it needs to transfer an emergency call. It sends a REFER via the I-CSCF to the ECT AS with a To header field set to the callback URI associated with the emergency caller, a Refer-To header field set to the transfer-to legacy PSAP URI, a Referred-By header field set to the transfer-from i3 PSAP URI, and an escaped Call-Info header containing a reference URI that points to the EIDO data structure and a purpose parameter of "eido". The REFER request is sent in the existing dialog between the caller and the transfer-from i3 PSAP.

After determining that the transfer-from PSAP is allowed to transfer calls, the ECT AS generates an ECT session identifier URI, addressed to itself, and replaces the Refer-To header field value with the ECT session identifier URI. This ensures that the ECT AS will remain in the path.

**Step 2.** The ECT AS forwards the REFER to the caller's UE via IBCFs at the edge of the Emergency Services Network and at the edge of the originating network (not shown).

**Step 3.** The caller's UE accepts the REFER request and returns a 200 OK to the ECT AS via IBCFs at the edge of the Emergency Services Network and at the edge of the originating network (not shown).

**Step 4.** The ECT AS forwards the 200 OK via an IBCF (not shown) toward the transfer-from i3 PSAP.

**Step 5.** The caller's UE sends a NOTIFY toward the ECT AS via IBCFs (not shown).

**Step 6.** The ECT AS sends a NOTIFY towards the transfer-from i3 PSAP via an IBCF (not shown).

**Step 7.** The transfer-from i3 PSAP sends a 200 OK back to the ECT AS via an IBCF (not shown).

**Step 8.** The ECT AS forwards the 200 OK to the caller's UE via IBCFs (not shown).

**Step 9.** The caller's UE initiates a call establishment toward the transfer-to legacy PSAP by sending a SIP INVITE message via the I-CSCF to the ECT AS. The INVITE message includes the ECT AS URI, the callback URI, and the Call-Info header received in the REFER.

**Step 10.** The ECT AS returns a 100 TRYING message to the caller's UE.

**Step 11.** The ECT AS forwards the INVITE via an IBCF (not shown) toward the LPG.

**Step 12.** The LPG returns a 100 TRYING message to the ECT AS.

**Step 13.** The caller's UE sends a NOTIFY message to the ECT AS to report the progress of the REFER request.

**Step 14.** The ECT AS sends a NOTIFY message to the transfer-from i3 PSAP to report the progress of the REFER request.

**Step 15.** The transfer-from i3 PSAP returns a 200 OK to the ECT AS in response to the NOTIFY message.

**Step 16.** The ECT AS returns a 200 OK message to the caller's UE.

**Step 17.** The LPG determines, based on provisioning, whether the transfer-to PSAP supports a Traditional MF or Enhanced MF interface. Depending on the type of interface supported by the PSAP, the LPG may generate a pANI and will assign an appropriate NPD or ANI II value to the call, following the procedures specified in Clause 6.2.2 of NENA-STA-010.3 [Ref 27].

**Step 18.** The LPG generates an off-hook signal toward the legacy PSAP.

**Step 19.** The legacy PSAP returns a wink signal back to the LPG.

**Step 20.** The LPG generates a 183 Session Progress message and sends it to the ECT AS (via an IBCF [not shown]).

**Step 21.** The ECT AS returns a 183 Session Progress message to the caller's UE.

**Step 22.** The caller's UE sends a NOTIFY message to the ECT AS to report the progress of the REFER request.

**Step 23.** The ECT AS sends a NOTIFY message to the transfer-from i3 PSAP to report the progress of the REFER request.

**Step 24.** The transfer-from i3 PSAP returns a 200 OK to the ECT AS in response to the NOTIFY message.

**Step 25.** The ECT AS returns a 200 OK message to the caller's UE.

**Step 26.** The LPG delivers the call to the legacy PSAP, mapping the SIP signaling from the incoming INVITE message to the outgoing Traditional or Enhanced MF signaling sequences, as appropriate for the legacy PSAP.

**Step 27.** Audible ringing is returned by the legacy PSAP to the LPG.

**Step 28.** Audible ringing is passed by the LPG to the caller's UE.

**Step 29.** When the PSAP answers the call, it returns an off-hook signal to the LPG.

**Step 30.** The LPG returns a 200 OK message to the ECT AS (via an IBCF [not shown]).

**Step 31.** The ECT AS passes the 200 OK message to the caller's UE (via an IBCF [not shown]).

**Step 32.** The caller's UE acknowledges receipt of the 200 OK by returning an ACK to the ECT AS (via an IBCF [not shown]).

**Step 33.** The ECT AS acknowledges receipt of the 200 OK message by returning an ACK to the LPG (via an IBCF [not shown]).

*RTP media is now flowing between the caller's UE and the LPG and voice media is flowing between the LPG and the transfer-to legacy PSAP.*

**Step 34.** The caller's UE sends a NOTIFY message to the ECT AS to report the progress of the REFER request.

**Step 35.** The ECT AS sends a NOTIFY message to the transfer-from i3 PSAP to report the progress of the REFER request.

**Step 36.** The transfer-from i3 PSAP returns a 200 OK to the ECT AS in response to the NOTIFY message.

**Step 37.** The ECT AS returns a 200 OK message to the caller's UE.

**Step 38.** The legacy PSAP sends a location query to the LPG using a legacy ALI protocol.

**Step 39.** The LPG queries the transfer-from i3 PSAP for the EIDO by including the URI provided in the Call-Info header in Step 11 in a GET request.

**Step 40.** The transfer-from PSAP returns the EIDO to the LPG.

**Step 41.** The LPG returns an ALI response to the legacy PSAP that includes the initial caller location information, a callback number and other information (e.g., class of service), as appropriate for the interface.

**Step 42.** Once the transfer-from i3 PSAP has determined that the call between the caller and the transfer-to i3 PSAP is active, it sends a BYE message to the ECT AS, terminating the original emergency dialog.

**Note:** Unlike the procedures defined in 3GPP TS 24.629 [Ref 49], which specify that a BYE will be sent by the transfer-from party after the REFER request has been accepted, the transfer-from PSAP must wait until it receives a notification that a 200 OK has been returned by the LPG (see Step 35) before sending a BYE message to terminate the dialog with the caller. This is necessary in the context of emergency services to ensure that a connection to the caller is maintained even if the transfer is unsuccessful.

**Step 43.** The ECT AS passes the BYE message associated with the original emergency dialog to the caller's UE.

**Step 44.** The caller's UE responds by returning a 200 OK to the ECT AS.

**Step 45.** The ECT AS returns a 200 OK to the transfer-from PSAP.

*Media between the caller and the transfer-from i3 PSAP is terminated.*

## 8.9 Policy Routing Scenarios

In certain scenarios it is desirable for an emergency call to be routed to a different destination than the one associated with the Route URI provided by the RDF as a result of performing location-based routing. In an IMS-based NG9-1-1 Service Architecture, the initial PSAP URI returned by the RDF to the LRF may be overwritten with another PSAP URI based on the policy routing rules specified by the PSAP or the 9-1-1 Authority and provisioned in the Policy Routing Function (PRF). After the LRF receives routing instructions (i.e., a Route URI) from the RDF, it interrogates the PRF with the Route URI to determine if there are policy routing rules associated with that URI. Based on the policy routing rules, the PRF may obtain an alternate URI to be used in routing the emergency call. The Route URI that results from the application of location-based and policy-based routing is returned to the E-

CSCF. The E-CSCF has no knowledge of whether the PSAP URI returned by LRF is the original one returned by the RDF or an alternate one determined by the PRF.

Policy routing allows for conditions/criteria other than location to be used in determining the routing of emergency calls. Routing decisions will be based on pre-provisioned policy rules that specify the conditions or decision criteria that should be considered (e.g., time-of-day) and the associated action that should be taken (e.g., alternate route for the call). Some of the reasons for routing a call to an alternate PSAP could be:

- PSAP maintenance.
- PSAP state.
- Additional data associated with the call, caller or location.
- Type of call (voice, text, video, etc.)
- Pre-definition of disaster routing.
- PSAP operating hours (time of day or day of the week).

The LRF uses the Policy Routing Rules within its PRF to make policy-based call routing decisions to support the delivery of a call to a PSAP. Policy Routing Rules allow 9-1-1 Authorities to address a wide range of operational situations to ensure 9-1-1 calls are delivered to a PSAP that can provide assistance consistent with established mutual aid agreements. See NENA-INF-011.2-2020 [Ref 51] for further discussion of operational considerations associated with the use of Policy Routing Rules.

The following example illustrates how Policy Rules may be used within a PSAP routing policy:

```
IF <condition = true> THEN <perform this Action>

IF <condition 1> THEN <route to PSAP A>
IF <condition 2> THEN <route to PSAP B>
IF <condition 3> THEN <route to PSAP C>
```

Example:

```
IF (time of day >1800 OR <= 0500) THEN <route to PSAP C> //deliver the calls to PSAP-C, single shift PSAP
                                                          Between 6pm – 5am hours.
```

The call flow in Figure 8-43 illustrates an example of call routing to an alternate PSAP due to policies enforced by the PRF. The call flow shows that the call was originally intended to be delivered to PSAP-A by the RDF based on the UE location. However due to PRF policies it was determined that the call cannot be delivered to PSAP-A, but instead must be delivered to PSAP-B. Thus the LRF/PRF returns the PSAP-B URI in the 300 Multiple Choices Response to E-CSCF. The E-CSCF forwards the call to PSAP-B via an IBCF.

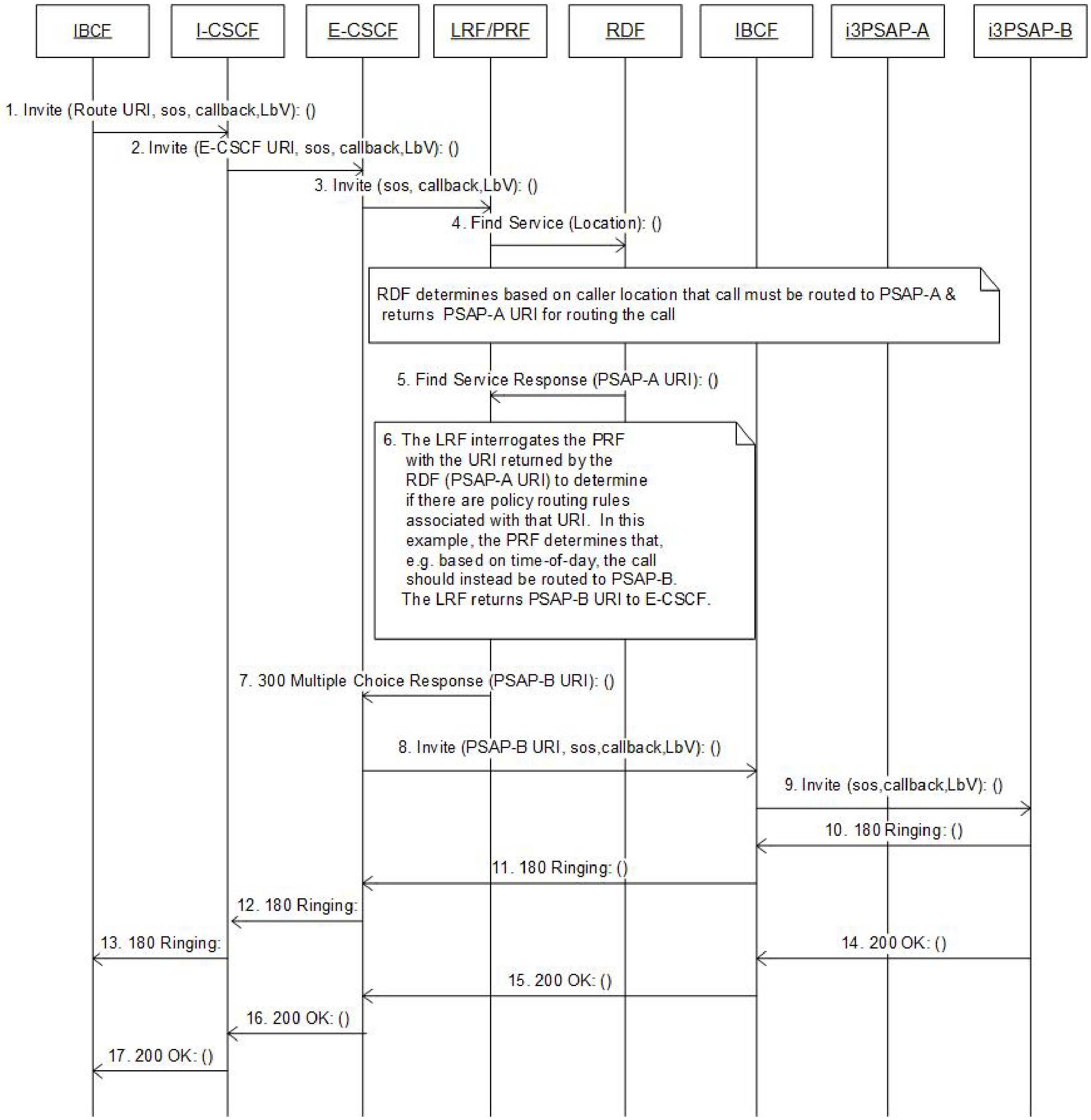

IBCF
I-CSCF
E-CSCF
LRF/PRF
RDF
IBCF
i3PSAP-A
i3PSAP-B
1. Invite (Route URI, sos, callback,LbV): ()
2. Invite (E-CSCF URI, sos, callback,LbV): ()
3. Invite (sos, callback,LbV): ()
4. Find Service (Location): ()
RDF determines based on caller location that call must be routed to PSAP-A & returns PSAP-A URI for routing the call
5. Find Service Response (PSAP-A URI): ()
6. The LRF interrogates the PRF with the URI returned by the RDF (PSAP-A URI) to determine if there are policy routing rules associated with that URI. In this example, the PRF determines that, e.g. based on time-of-day, the call should instead be routed to PSAP-B. The LRF returns PSAP-B URI to E-CSCF.
7. 300 Multiple Choice Response (PSAP-B URI): ()
8. Invite (PSAP-B URI, sos,callback,LbV): ()
9. Invite (sos,callback,LbV): ()
10. 180 Ringing: ()
11. 180 Ringing: ()
12. 180 Ringing:
13. 180 Ringing:
14. 200 OK: ()
15. 200 OK: ()
16. 200 OK: ()
17. 200 OK: ()

**Figure 8.44: IMS Based Call to i3 PSAP – PRF Example**

**Step 1.** The IBCF in IMS-based NG9-1-1 Emergency Services Network forwards the incoming SIP INVITE message from IMS Originating network to the I-CSCF. The SIP INVITE message includes a Route header that contains the I-CSCF URI, an emergency services service URN (urn:service:sos), callback information, LbyV, and Additional Data (by value).

**Step 2.** The I-CSCF forwards the SIP INVITE to the pre-configured E-CSCF. The SIP INVITE message sent to the E-CSCF by the I-CSCF contains the E-CSCF URI in the Route header, and includes the callback information, “sos” service URN and LbyV, as received in the incoming SIP INVITE message.

**Step 3.** The E-CSCF forwards the SIP INVITE to the LRF.

**Step 4.** The LRF queries the RDF using the location information received in the body of the received SIP INVITE message.

**Step 5.** The RDF returns a Route URI. In this example, the Route URI is associated with an i3 PSAP-A that is served by the IMS-based NG9-1-1 Emergency Services Network.

**Step 6.** The LRF interrogates the PRF with the URI returned by the RDF (PSAP-A URI) to determine if there are policy routing rules associated with that URI. In this example, the PRF determines that, e.g., based on time-of-day, the call should instead be routed to PSAP-B. The LRF returns PSAP-B URI to E-CSCF.

**Step 7.** The LRF redirects the call back to E-CSCF by sending 300 Multiple Choice Response, passing the Route URI for PSAP-B.

**Step 8.** The E-CSCF generates an outgoing SIP INVITE message, using the information received from the LRF as well as information received in the initial SIP INVITE message, and forwards it to the IBCF.

**Step 9.** The IBCF forwards the SIP INVITE to the i3 PSAP-B with the callback information, the LbyV, and the Additional Data received in the initial SIP INVITE message from the IMS originating network.

**Step 10.** An indication that the call taker is being alerted is returned by the i3 PSAP to the IBCF (using a SIP 180 RINGING message).

**Step 11.** The IBCF passes the SIP 180 RINGING message to the E-CSCF.

**Step 12.** The E-CSCF passes the SIP 180 RINGING message to the I-CSCF.

**Step 13.** The I-CSCF passes the SIP 180 RINGING message to the IBCF.

**Step 14.** When the PSAP answers the call, it returns a SIP 200 OK message to the IBCF.

**Step 15.** The IBCF passes the SIP 200 OK message to the E-CSCF.

**Step 16.** The E-CSCF passes the SIP 200 OK message to the I-CSCF.

**Step 17.** The I-CSCF passes the SIP 200 OK message to the IBCF.

## *8.10 Failure Scenarios*

This clause discusses some of the potential error cases that may be encountered during call set up and once the call is completed. It is not intended to be an exhaustive list of error cases, but highlights example scenarios.

This standard does not address the deployment of redundant functional elements, but it is assumed that the critical network elements will be redundant or deployed in an N+1 configuration. Given such a configuration, if a network element attempts to communicate with a downstream network element and detects an error (e.g., timeout) it should attempt to communicate with the redundant downstream network element. For example, if the I-CSCF and E-CSCF are deployed in separate physical units and the I-CSCF attempts to forward the SIP INVITE to the E-CSCF and encounters a timeout, it should attempt to forward the SIP INVITE to the redundant E-CSCF. This applies to all of the following error cases, but the error cases below describe action where there is a complete communication failure or the data is not available or corrupted.

### 8.10.1 Error Conditions

Upon encountering the following error conditions, it may not be possible to obtain location, identify the primary PSAP or determine the appropriate PSAP signaling format. Clause 9.2.2 defines optional error handling for calls entering the IMS-based NG9-1-1 Emergency Services Network via SS7. If that is not implemented, the following handling applies. Except as noted, the recommended treatment for these scenarios is to forward the call to a default destination (e.g., a call center) to allow a human to determine how best to process the call.

- E-CSCF does not get a 300 Multiple Choices response from the LRF.

In this scenario the E-CSCF does not have sufficient information to determine the primary PSAP and the appropriate signaling method to route the call. The E-CSCF should route the call to a default destination (e.g., PSAP or call center).

- The LRF does not get a response from the LS.

There are two scenarios related to this condition: routing a fixed location call and routing a wireless call that uses associated location.

  - Fixed Location call.

Without the location the LRF cannot query the RDF to determine the primary PSAP. It should return a Route URI in the 300 Multiple Choices response that allows the E-CSCF to route the call to a default destination.

  - Wireless call routed using associated location.

If the LRF determines call routing using the associated location, then it can do so without a response from the LS. The LRF should return a Route URI in the 300 Multiple Choices response that allows the E-CSCF to route the call to a default destination.

  - If the LRF is unable to determine an associated location, it should return a Route URI in the 300 Multiple Choices response that allows the E-CSCF to route the call to a default destination.

- The LRF does not get a response from the RDF.

If the LRF does not get a response from the RDF it cannot determine the primary PSAP. It should return a Route URI in the 300 Multiple Choices response that allows the E-CSCF to route the call to a default destination.

- The E-CSCF gets an error in its attempt to forward the SIP INVITE toward the PSAP.

If the E-CSCF is unable to complete the dialogue with the primary PSAP it should redirect the call to a default destination.

## *8.11 PSAP Callback Flows*

Multimedia callback calls from i3 PSAPs are expected to transit an IMS-based NG9-1-1 Emergency Services Network. The Transit Function within the IMS-based NG9-1-1 Emergency Services Network will be responsible for taking a callback call originated by an i3 PSAP and delivering it to an interconnected network (i.e., a directly connected emergency caller's network or transit network) which will ultimately forward the call to/toward the emergency caller's device. As described in 3GPP TS 23.228 [Ref 19], the Transit Function is an element that determines where to route a session based on an analysis of the destination address. This includes routing to destinations in other IMS networks or the PSTN. The IMS-based NG9-1-1 Emergency Services Network must have an IP-based Network-to-Network Interface (NNI) to one or more interconnected networks to facilitate callbacks routed using the Transit Function. An i3 PSAP that initiates a callback call will send a SIP INVITE towards the IMS-based NG9-1-1 Emergency Services Network via a BCF and IBCF. The SIP INVITE message must contain the following information:

- A Request-URI line containing the callback URI;
- A To header field populated with the callback URI, as received in the P-Asserted-Identity (preferred, if present) or From header field of the original emergency call;

  Note: The callback URI must contain a dialable telephone number either expressed as a national 10-digit NANP number or as an international number following ITU-T Recommendation E.164 and, if expressed as a sip URI, the domain part shall represent the home network of the target. If the original emergency call was from a non-service initialized handset, the callback number of the form “911 plus the last 7 digits of the ESN or IMEI expressed as a decimal” is not dialable and therefore must not be used for callback.
- A From header field containing sip:TN@<psapdomain>;user=phone, which should be the same value as in the P-Asserted-Identify header field;

Note: The IMS-based NG9-1-1 Emergency Services Network must support receipt of outgoing calls from PSAPs marked for presentation restriction of caller ID expressed by the presence of a Privacy header field (RFC 3323 [Ref 45], expanded by RFC 3325 [Ref 46] and RFC 7044 [Ref 47]) and the From header field value populated with "Anonymous" (i.e., sip:anonymous@anonymous.invalid);

- A Route header field containing the Transit Function URI. (Note that the INVITE from the Transit Function to the interconnected network shall contain the well-known URI associated with that network);
- A SIP Priority header field with “psap-callback” as the value;
- A Resource-Priority header field with “esnet.0” as the value;
- A P-Asserted-Identity header field containing sip:TN@<psapdomain>;user=phone, where the TN is associated with the PSAP originating the call;
- A second P-Asserted-Identity header field containing the identity of the agent originating the call expressed as sip: “agent name” <agentID@agencyID>;

  Note: the Display Name part is OPTIONAL;
- An SDP offer containing all media supported at the PSAP. The SDP should include offers matching the negotiated SDP from the original emergency call, placing the SDP that was used as the top-most value in the list;

Upon receiving the SIP INVITE message from the i3 PSAP (via the BCF), the entry point IBCF applies general screening rules to the request and adds the orig parameter to the INVITE to indicate that this is an origination request. It then sends the INVITE directly to the Transit Function. The Transit Function uses the destination address (i.e., the callback URI) in the Request-URI to determine the routing for the call. If the call is destined for an interconnected IP network, the Transit Function forwards the call to the exit point IBCF. If the IMS-based NG9-1-1 Emergency Services Network supports the authentication architecture described in Clause 7.3.2.1, then before forwarding the call to the exit point IBCF, the Transit Function forwards the request to the STI-AS for authentication of the calling party as identified in the P-Asserted-Identity header (e.g., sip:TN@<psapdomain>;user=phone, where the TN is associated with the PSAP originating the call) and signing of the RPH and SIP Priority header. The STI-AS determines, through service provider-specific means, the legitimacy of the telephone number identity and the RPH and SIP Priority header values being used in the INVITE. The STI-AS then securely requests its private key from the SKS. The SKS provides the private key in the response, and the STI-AS signs the INVITE and adds an Identity header field per RFC 8224 [Ref 36] using the caller identity in the P-Asserted-Identity header field and an Identity header associated with the signed RPH/SIP Priority header. (See Clauses 7.3.2.1 and 7.4 for further details.) The STI-AS passes the INVITE back to the Transit Function. The Transit Function routes the call to the exit point IBCF. The SIP INVITE is routed over the NNI through the standard inter-domain routing configuration toward the entry point IBCF associated with the emergency caller’s home network. See Clauses 8.12.3 and 8.12.5 for example call flows.

If the IMS-based NG9-1-1 Emergency Services Network supports the authentication architecture described in Clause 7.3.2.2, then upon receiving the SIP INVITE message from the Transit Function, the exit point IBCF sends an HTTP POST containing a signingRequest associated with the caller identity and a signingRequest associated with the RPH/SIP Priority header to the STI-AS for signing of the caller identity as identified in the P-Asserted-Identity header (e.g., sip:TN@<psapdomain>;user=phone, where the TN is associated with the PSAP originating the call) and the RPH/SIP Priority header. The STI-AS determines, through service provider-specific means, the legitimacy of the telephone number identity and the RPH and SIP Priority header provided in the signing requests. The STI-AS then securely requests its private key from the SKS. The SKS provides the private key in the response, and the STI-AS signs the caller identity and RPH/SIP Priority header and returns an HTTP 200 OK that includes a signingResponse that contains an identityHeader parameter associated with the caller identity and a signingResponse that contains an identityHeader parameter associated with the RPH/SIP Priority header. (See Clauses 7.3.2.2 and 7.4 for further details.) The exit point IBCF uses the identityHeader parameters to populate SIP Identity header fields in the outgoing INVITE message and routes the call over the NNI using standard inter-domain routing toward the entry point IBCF associated with the emergency caller’s home network. See Clauses 8.12.4 and 8.12.6 for example call flows.

## *8.12 Caller Identity and Resource-Priority Header Authentication/Signing and Verification*

The following call flows illustrate the application of the STI authentication and verification procedures to 9-1-1 and callback calls using the architectures described in Clause 7.3, and the RPH and SIP Priority header signing/verification procedures described in Clause 7.4. These call flows consider 9-1-1 calls that originate in IMS-based and non-IMS IP-based originating networks and are delivered to IMS-based NG9-1-1 Emergency Services Networks, as well as callback calls from i3 PSAPs that are routed via an IMS-based NG9-1-1 Emergency Services Network to an IMS-based or non-IMS IP-based emergency caller's home network. The callback call flows consider both an architecture in which a Transit Function in the NG9-1-1 Emergency Services Network interacts with an STI-AS, as well as an architecture where the exit IBCF in an NG9-1-1 Emergency Services Network interacts with the STI-AS.

### 8.12.1 9-1-1 Origination from an IMS Originating Network

In this call flow, the emergency call is processed by an IMS originating network. Location-based routing performed by the originating network determines that the emergency call is to be routed via an IMS-based NG9-1-1 Emergency Services Network. The exit IBCF in the IMS originating network interacts with the STI-AS to request signing of the caller identity and the RPH. Upon receiving signing responses from the STI-AS with identityHeader parameters associated with the signed caller identity and RPH, the exit IBCF creates and populates Identity headers in the outgoing SIP INVITE message and forwards the SIP INVITE message to the entry IBCF in the IMS-based NG9-1-1 Emergency Services Network. The entry IBCF interacts with an STI-VS to request verification of the received Identity headers. The STI-VS returns the verification results to the entry IBCF. The entry IBCF populates those results in the SIP INVITE message and forwards the SIP INVITE message to the I-CSCF using the procedures specified in this document. Call processing continues according to the procedures specified elsewhere in this document, with the caller identity and associated verification results conveyed to the i3 PSAP's call handling equipment (or the LPG) in the P-Asserted-Identity header, the attestation information conveyed in the Identity header, the signed RPH, and the verification results associated with the RPH in a Priority-Verstat header field.

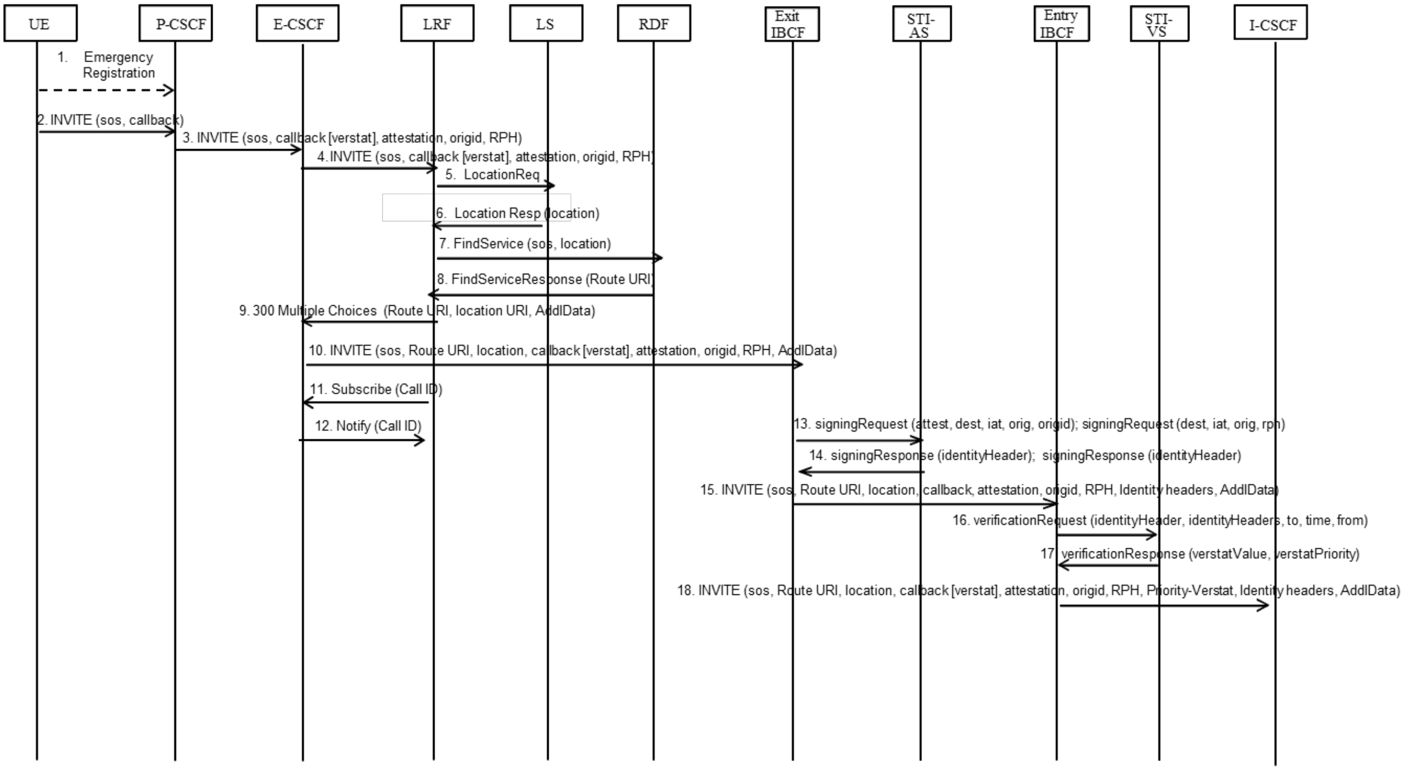

UE
P-CSCF
E-CSCF
LRF
LS
RDF
Exit IBCF
STI-AS
Entry IBCF
STI-VS
I-CSCF
1. Emergency Registration
2. INVITE (sos, callback)
3. INVITE (sos, callback [verstat], attestation, origid, RPH)
4. INVITE (sos, callback [verstat], attestation, origid, RPH)
5. LocationReq
6. Location Resp (location)
7. FindService (sos, location)
8. FindServiceResponse (Route URI)
9. 300 Multiple Choices (Route URI, location URI, AddlData)
10. INVITE (sos, Route URI, location, callback [verstat], attestation, origid, RPH, AddlData)
11. Subscribe (Call ID)
12. Notify (Call ID)
13. signingRequest (attest, dest, iat, orig, origid); signingRequest (dest, iat, orig, rph)
14. signingResponse (identityHeader); signingResponse (identityHeader)
15. INVITE (sos, Route URI, location, callback, attestation, origid, RPH, Identity headers, AddlData)
16. verificationRequest (identityHeader, identityHeaders, to, time, from)
17. verificationResponse (verstatValue, verstatPriority)
18. INVITE (sos, Route URI, location, callback [verstat], attestation, origid, RPH, Priority-Verstat, Identity headers, AddlData)

**Figure 8-44: IMS Emergency Call Origination with Caller Identity and RPH Signing/Verification**

**Step 1.** (Conditional) Emergency registration occurs (if not already emergency registered and has credentials).

**Step 2.** The originating SIP UE, which is authenticated to the P-CSCF, creates a SIP INVITE with a callback number (i.e., a telephone number identity) and an sos service URN in the Request URI.

**Step 3.** The P-CSCF in the originating network adds a P-Asserted-Identity header field asserting the callback number/caller identity of the originating SIP UE and an RPH with a value of “esnet.1”. If supported by local policy, the P-CSCF will also insert a verstat parameter in the P-Asserted-Identity header, and optional Attestation-Info and Origination-Id header fields in the SIP INVITE message for use by downstream calling identity authentication and verification processes. The P-CSCF passes the SIP INVITE to the E-CSCF.

**Step 4.** The E-CSCF passes the SIP INVITE message to the LRF to obtain location and routing information for the emergency call.

**Step 5.** The LRF selects a technique for acquiring location information based upon the call type. The LRF interacts with an LS to acquire location/initiate position determination, as applicable.

**Step 6.** The LS responds with location information.

**Step 7.** The LRF queries the RDF using the location information and an sos service URN.

**Step 8.** The RDF returns a Route URI. In this example, the Route URI is associated with an I-CSCF in an IMS-based NG9-1-1 Emergency Services Network.

**Step 9.** The LRF redirects the call back to the E-CSCF by returning a 300 Multiple Choices message that contains location information, a Route URI that directs the call toward the IMS-based NG9-1-1 Emergency Services Network, and Additional Data.

**Step 10.** The E-CSCF generates an outgoing SIP INVITE message, using the information received from the LRF as well as information received in the initial SIP INVITE message, and forwards it to the exit IBCF. In this example the SIP INVITE includes the sos service URN, a Route URI, location information, the callback number with associated verstat information, an Attestation-Info header, an Origination-Id header, the RPH, and Additional Data.

**Step 11.** The LRF sends a SIP SUBSCRIBE to the E-CSCF to be informed of call state. (Alternatively, the Subscription may be done at the system start-up and be applicable to all calls [not shown].)

**Step 12.** The E-CSCF sends an initial state NOTIFY to the LRF.

**Step 13.** The exit IBCF sends an HTTP POST containing two signing requests over the Ms reference point to the STI-AS. The signingRequest associated with the caller identity includes an “attest” parameter that contains the attestation information received by the IBCF in the Attestation-Info header in the SIP INVITE, as well as other PASSporT information (i.e., “orig”, “dest”, “iat” and “origid”). The second signingRequest includes the “rph” claim, as described in Clause 7.4, as well as the “orig”, “dest” and “iat”. This call flow assumes that the exit IBCF populates an “auth” key with an assertion value of “esnet.1” in the “rph” claim based on receipt of the RPH.

**Step 14.** The STI-AS first determines through service provider-specific means the legitimacy of the telephone number identity and RPH being used in the INVITE. The STI-AS securely requests its private key from the SKS, and the SKS provides the private key in response (not shown). The STI-AS then returns an HTTP 200 OK message that includes a signingResponse that contains the signed identityHeader parameter associated with the caller identity and a signingResponse that contains the signed identityHeader associated with the RPH.

**Step 15.** The exit IBCF uses the information returned in the identityHeader parameters to populate SIP Identity headers associated with the caller identity (callback number) and the RPH in the SIP INVITE message. The IBCF also removes the verstat (if present) prior to sending the call to the NG9-1-1 Emergency Services Network. The exit IBCF then routes the SIP INVITE over the NNI to the entry IBCF in the IMS-based NG9-1-1 Emergency Services Network using standard inter-domain routing resolution.

**Step 16.** Upon receiving the SIP INVITE, the ingress IBCF in the NG9-1-1 Emergency Services Network sends an HTTP POST containing a verificationRequest to the STI-VS. The verificationRequest includes an “identityHeader” parameter corresponding to the Identity header containing the signed caller identity information, an “identityHeaders” parameter corresponding to the Identity header containing the signed RPH information, as well as the “to” parameter containing the destination identity from the To header, the “from” parameter containing the asserted identity from the From or P-Asserted-Identity, and a “time” parameter based on the Date header field in the incoming request.

**Step 17.** The STI-VS determines the STI-CR Uniform Resource Identifier (URI) and makes an HTTPS request to the STI-CR (not shown). The STI-VS validates the certificate and then extracts the public key. It uses the public key to verify the signature in the “identityHeader” and “identityHeaders” parameters, which validate the caller identity and RPH content signed by the originating network STI-AS. The STI-VS may interact with the CVT based on local policy and agreements between the 9-1-1 Authority and the analytics/CVT provider. The STI-VS returns an HTTP 200 OK containing a verificationResponse to the ingress IBCF. The verificationResponse contains a “verstatValue” parameter associated with the “identityHeader” parameter in the verificationRequest and a “verstatPriority” parameter associated with the “rph” claim in the “identityHeaders” parameter in the verificationRequest, indicating the result of the verification process. Depending on the results of the verification process, the “verstatValue” associated with the signed caller identity will be set to “TN-Validation-Passed”, “TN-Validation-Failed”, or “No-TN-Validation”, and the “verstatPriority” associated with the signed RPH will be set to “RPH-Validation-Passed”, “RPH-Validation-Failed”, or “No-RPH-Validation”.

**Step 18.** The ingress IBCF passes the INVITE to the I-CSCF in the NG9-1-1 Emergency Services Network. In this example the SIP INVITE includes the sos service URN, a Route URI, location information, the callback number with associated verstat information (populated as a parameter in the P-Asserted-Identity header), an Attestation-Info header, an Origination-Id header, the RPH and associated verification status information (populated in a Priority-Verstat header field), the Identity headers, and Additional Data.

### 8.12.2 9-1-1 Origination from a Non-IMS VoIP Originating Network

In this call flow, the emergency call is processed by a non-IMS IP-based originating network. Location-based routing performed by the originating network determines that the emergency call is to be routed via an IMS-based NG9-1-1 Emergency Services Network. The Call Server/Proxy in the originating network passes the SIP INVITE message associated with the emergency call to the STI-AS for attestation/authentication of the caller identity and signing of the RPH. Upon receiving the SIP INVITE back from the STI-AS with Identity headers associated with the signed caller identity and RPH, the Call Server/Proxy passes the SIP INVITE message (via a BCF/Session Border Controller (SBC) [not shown]) to the entry IBCF in the IMS-based NG9-1-1 Emergency Services Network. The entry IBCF interacts with an STI-VS to request verification of the received Identity headers. The STI-VS returns the verification results to the entry IBCF. The entry IBCF populates those results in the SIP INVITE message and forwards the SIP INVITE message to the I-CSCF using the procedures specified in this document. Call processing continues according to the procedures specified elsewhere in this document, with the caller identity and associated verification results conveyed to the i3 PSAP’s call handling equipment (or the LPG) in the P-Asserted-Identity header, the attestation information conveyed in the Identity header, the signed RPH, and the verification results associated with the RPH in a Priority-Verstat header field.

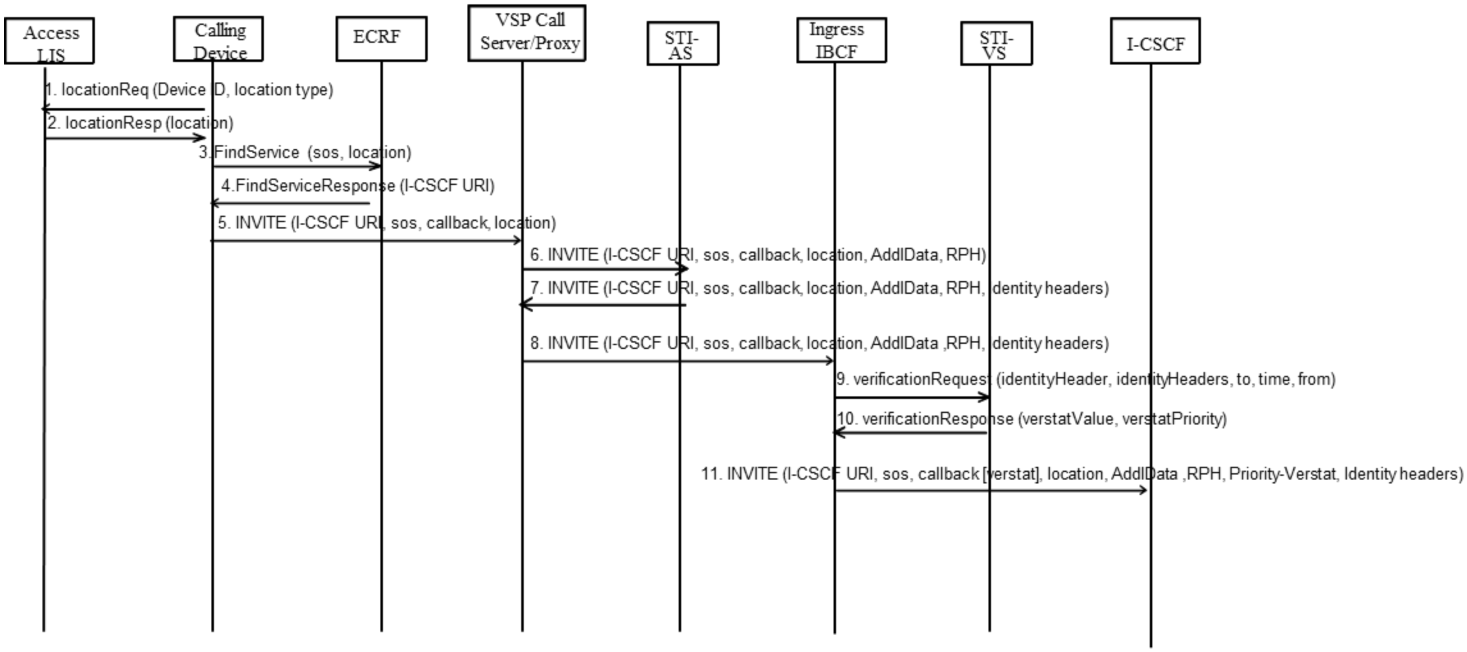

Access LIS
Calling Device
ECRF
VSP Call Server/Proxy
STI-AS
Ingress IBCF
STI-VS
I-CSCF
1. locationReq (Device ID, location type)
2. locationResp (location)
3.FindService (sos, location)
4.FindServiceResponse (I-CSCF URI)
5. INVITE (I-CSCF URI, sos, callback, location)
6. INVITE (I-CSCF URI, sos, callback, location, AddlData, RPH)
7. INVITE (I-CSCF URI, sos, callback, location, AddlData, RPH, Identity headers)
8. INVITE (I-CSCF URI, sos, callback, location, AddlData ,RPH, Identity headers)
9. verificationRequest (identityHeader, identityHeaders, to, time, from)
10. verificationResponse (verstatValue, verstatPriority)
11. INVITE (I-CSCF URI, sos, callback [verstat], location, AddlData ,RPH, Priority-Verstat, Identity headers)

**Figure 8-45: Non-IMS Emergency Call Origination with Caller Identity and RPH Signing/Verification**

**Step 1.** Upon recognizing a request for emergency service, the calling device requests location by querying the LIS in the access network. (This example illustrates the use of the HELD protocol for the location request.) The locationRequest contains an identifier and appropriate credentials associated with the calling device, as well as an indication of the type of location being requested. In this example, the device requests civic or geodetic location. The locationRequest also includes a responseTime parameter (not shown) indicating how long the device is prepared to wait for a response or the purpose for which the device needs the location.

**Step 2.** The LIS responds to the location request by returning location information.

**Step 3.** The device uses the location returned by the LIS and the emergency service URN (urn:service:sos) to query an ECRF for routing information.

**Step 4.** The ECRF responds by returning a URI associated with an I-CSCF in an IMS-based NG9-1-1 Emergency Services Network.

**Step 5.** The device generates a SIP INVITE message that includes a Route header that contains the I-CSCF URI, an emergency services service URN (urn:service:sos), callback information, and location information, and sends it to a Call Server/Proxy in its serving non-IMS originating network.

**Step 6.** The Call Server/Proxy adds Additional Data “by value” to the received SIP INVITE message by including a Call-Info header that contains a cid pointing to the Additional Data in the message body. The Call Server/Proxy also adds an RPH with a value of “esnet.1” to the SIP INVITE message and forwards it to an STI-AS.

**Step 7.** The STI-AS determines, through service provider-specific means, the legitimacy of the content of the caller identity and the RPH field. The STI-AS then securely requests its private key from the SKS (not shown). The STI-AS signs and adds Identity header fields to the SIP INVITE message and returns it to the Call Server/Proxy.

**Step 8.** The Call Server/Proxy forwards the SIP INVITE message (via a BCF/SBC [not shown]) to an IBCF on the ingress side of the IMS-based NG9-1-1 Emergency Services Network. The SIP INVITE message includes the I-CSCF URI, an emergency services service URN (urn:service:sos), callback information, location information, Additional Data, RPH, and Identity headers.

**Step 9.** Upon receiving the SIP INVITE, the ingress IBCF in the NG9-1-1 Emergency Services Network sends an HTTP POST containing a verificationRequest to the STI-VS. The verificationRequest includes an “identityHeader” parameter corresponding to the Identity header containing the signed caller identity information, an “identityHeaders” parameter corresponding to the Identity header containing the signed RPH information, as well as the “to” parameter containing the destination identity from the To header, the “from” parameter containing the asserted identity from the From or P-Asserted-Identity, and a “time” parameter based on the Date header field in the incoming request.

**Step 10.** The STI-VS determines the STI-CR Uniform Resource Identifier (URI) and makes an HTTPS request to the STI-CR (not shown). The STI-VS validates the certificate and then extracts the public key. It uses the public key to verify the signature in the “identityHeader” and “identityHeaders” parameters, which validate the caller identity and RPH content signed by the originating network STI-AS. The STI-VS may interact with the CVT based on local policy and agreements between the 9-1-1 Authority and the analytics/CVT provider. The STI-VS returns an HTTP 200 OK containing a verificationResponse to the ingress IBCF. The verificationResponse contains a “verstatValue” parameter (associated with the “identityHeader” parameter in the verificationRequest) and a “verstatPriority” parameter (associated with the “rph” claim in the “identityHeaders” parameter in the verificationRequest) that contain the results of the verification process. Depending on the results of the verification process, the “verstatValue” associated with the signed caller identity will be set to “TN-Validation-Passed”, “TN-Validation-Failed”, or “No-TN-Validation”, and the “verstatPriority” associated with the signed RPH will be set to “RPH-Validation-Passed”, “RPH-Validation-Failed”, or “No-RPH-Validation”.

**Step 11.** The ingress IBCF passes the INVITE to the I-CSCF in the NG9-1-1 Emergency Services Network. In this example the SIP INVITE includes the sos service URN, the I-CSCF URI, location information, the callback number with associated verstat information, the RPH, the Priority-Verstat header field (containing the verification status information associated with the signed RPH), the Identity headers, and Additional Data.

### 8.12.3 Callback to IMS Home Network - Transit Function Interacts with STI-AS

In this call flow example, an i3 PSAP initiates a callback call by sending a SIP INVITE that includes a To header and Request-URI that contains the callback number from the original emergency call, From and P-Asserted-Identity headers that contain the telephone number of the PSAP, “psap-callback” in the Priority header, and “esnet.0” in the Resource-Priority header, via a BCF (not pictured) to an entry IBCF in the IMS-based NG9-1-1 Emergency Services. The entry IBCF performs normal screening and passes the SIP INVITE to the Transit Function. In this call flow example, after determining that the call is to be directed to an IP-capable interconnecting network, the Transit Function forwards the SIP INVITE to the STI-AS. The STI-AS performs attestation and authentication of the caller identity information and signing of the RPH and SIP Priority header, then populates an Identity header associated with the caller identity and an Identity header associated with the signed RPH/SIP Priority header in the SIP INVITE and returns it to the Transit Function. The Transit Function then routes the callback call to an exit IBCF in the IMS-based NG9-1-1 Emergency Services Network which forwards the call via the NNI to an entry IBCF in the interconnecting network. This example assumes that the exit IBCF forwards the SIP INVITE to the entry IBCF in the emergency caller’s home network. Depending on the scenario, the callback call may traverse other interconnecting networks before reaching the emergency caller’s home network.

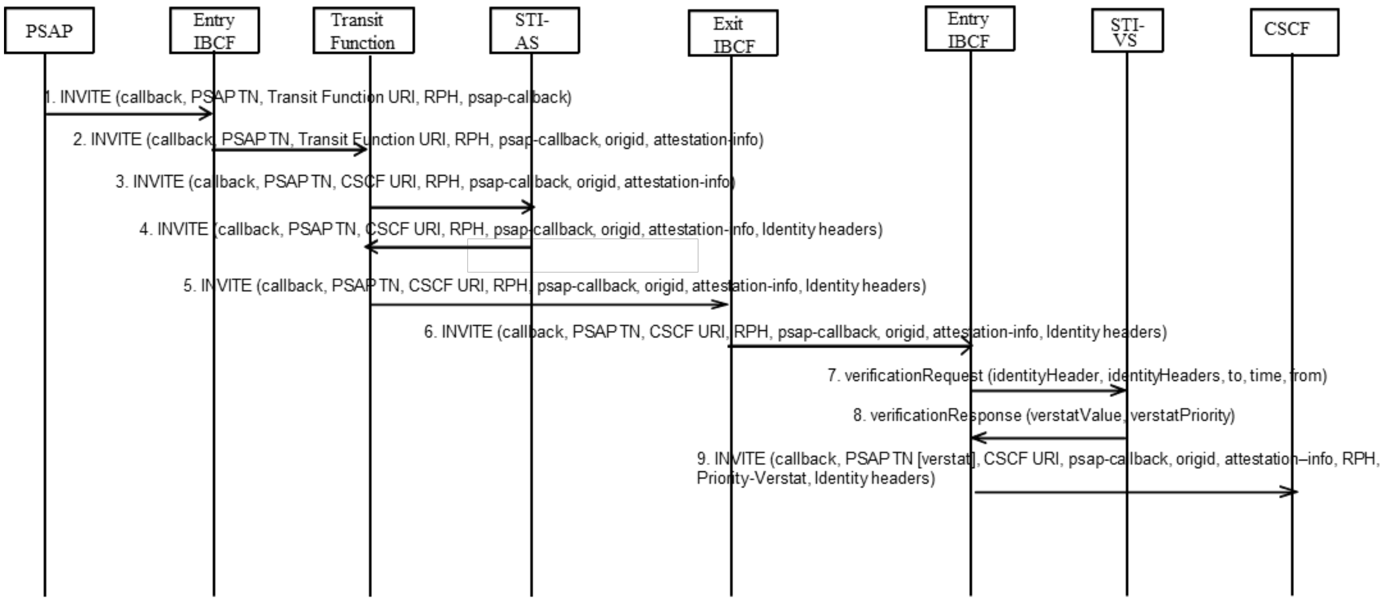

PSAP
Entry IBCF
Transit Function
STI-AS
Exit IBCF
Entry IBCF
STI-VS
CSCF
1. INVITE (callback, PSAP TN, Transit Function URI, RPH, psap-callback)
2. INVITE (callback, PSAP TN, Transit Function URI, RPH, psap-callback, origid, attestation-info)
3. INVITE (callback, PSAP TN, CSCF URI, RPH, psap-callback, origid, attestation-info)
4. INVITE (callback, PSAP TN, CSCF URI, RPH, psap-callback, origid, attestation- info, Identity headers)
5. INVITE (callback, PSAP TN, CSCF URI, RPH, psap-callback, origid, attestation-info, Identity headers)
6. INVITE (callback, PSAP TN, CSCF URI, RPH, psap-callback, origid, attestation-info, Identity headers)
7. verificationRequest (identityHeader, identityHeaders, to, time, from)
8. verificationResponse (verstatValue, verstatPriority)
9. INVITE (callback, PSAP TN [verstat], CSCF URI, psap-callback, origid, attestation–info, RPH, Priority-Verstat, Identity headers)

**Figure 8-46: Callback Call with Caller Identity and RPH Signing Initiated by Transit Function**

**Step 1.** The PSAP Call Handling Function initiates a callback call, generating a SIP INVITE message with the callback URI from the original emergency call in the To header and Request-URI, the TN of the PSAP originating the callback (i.e., sip:TN@<psapdomain>;user=phone) in the From and P-Asserted-Identity headers, "psap-callback" in the Priority header, and "esnet.0" in the Resource-Priority header. The PSAP Call Handling Function passes the SIP INVITE via a BCF (not shown) to an entry IBCF in an IMS-based NG9-1-1 Emergency Services Network.

**Step 2.** Upon receiving the SIP INVITE message, the entry IBCF applies general screening rules to the request, and based on local policy, adds an Origination-Id header to the INVITE to indicate from where the request was received, along with an Attestation-Info header. It then forwards the INVITE to the Transit Function.

**Step 3.** The Transit Function uses the destination address (i.e., the callback URI) in the Request-URI to determine the routing for the call. Before forwarding the call to the interconnecting network, the Transit Function sends the request to the STI-AS for authentication and signing of the caller identity and signing of the RPH and SIP Priority header.

**Step 4.** The STI-AS determines, through service provider-specific means, the legitimacy of the content of the caller identity and the RPH and SIP Priority header fields. The STI-AS then securely requests its private key from the SKS (not shown). Upon receiving the private key from the SKS, the STI-AS signs the caller identity and RPH/SIP Priority header and adds Identity header fields (one associated with the caller identity and one associated with the RPH/SIP Priority) to the SIP INVITE message. The STI-AS then returns the SIP INVITE, with the signed Identity headers, to the Transit Function.

**Step 5.** The Transit Function routes the SIP INVITE (with the Identity headers) to the exit IBCF.

**Step 6.** In this example, the exit IBCF forwards the SIP INVITE to the entry IBCF in the emergency caller's home network. Note that depending on the scenario, the callback call may traverse other interconnecting networks before reaching the emergency caller's home network. If, based on local policy, a verstat is present in the received SIP INVITE, the exit IBCF will remove the verstat before forwarding the call to the next network.

**Step 7.** The entry IBCF in the emergency caller's home network initiates an HTTP POST message to the STI-VS that includes a verificationRequest containing an "identityHeader" claim corresponding to the Identity header containing the signed caller identity information, an "identityHeaders" claim corresponding to the Identity header containing the signed RPH and

Priority header information, as well as a "to" parameter containing the destination identity from the To header, a "from" parameter containing the asserted identity from the From or P-Asserted-Identity, and a "time" parameter based on the Date header field in the incoming request.

**Step 8.** The STI-VS determines the STI-CR Uniform Resource Identifier (URI) and makes an HTTPS request to the STI-CR (not shown). The STI-VS validates the certificate and then extracts the public key. It uses the public key to verify the signature in the "identityHeader" and "identityHeaders" parameters, which validate the caller identity and the RPH and SIP Priority header content signed by the IMS-based NG9-1-1 Emergency Services Network STI-AS. The STI-VS may interact with the CVT based on local policy and agreements between the home network provider and the analytics/CVT provider. The STI-VS returns an HTTP 200 OK that contains a verificationResponse to the ingress IBCF. The verificationResponse contains a "verstatValue" parameter (associated with the "identityHeader" parameter in the verificationRequest) and a "verstatPriority" parameter (associated with the "rph" and "sph" claims in the "identityHeaders" parameter in the verificationRequest), indicating the result of the verification process. Depending on the results of the verification process, the "verstatValue" associated with the signed caller identity will be set to "TN-Validation-Passed", "TN-Validation-Failed", or "No-TN-Validation", and the "verstatPriority" associated with the signed RPH/SIP Priority header will be set to "ECB-RPH-Validation-Passed", "ECB-RPH-Validation-Failed", or "No-ECB-RPH-Validation".

**Step 9.** The entry IBCF continues to set up the callback call to the CSCF. The SIP INVITE message includes the callback number associated with the emergency caller, the PSAP telephone number and associated verstat parameter, the URI of the target CSCF, the RPH set to "esnet.0", a Priority header set to "psap-callback", a Priority-Verstat header field containing verification status information associated with the RPH/SIP Priority header, the Origination-Id, the Attestation-Info header, and the Identity headers.

### 8.12.4 Callback to IMS Home Network - Exit IBCF Interacts with STI-AS

In this call flow example, an i3 PSAP initiates a callback call by sending a SIP INVITE that includes a To header and Request-URI that contains the callback number from the original emergency call, From and P-Asserted-Identity headers that contain the telephone number of the PSAP, "psap-callback" in the Priority header, and "esnet.0" in the Resource-Priority header, via a BCF (not pictured) to an entry IBCF in the IMS-based NG9-1-1 Emergency Services Network. The entry IBCF performs normal screening and based on local policy, adds an Attestation-Info header and an Origination-Id header (to indicate from where the request was received) to the INVITE. The IBCF then passes the SIP INVITE to the Transit Function. In this call flow example, after determining that the call is to be directed to an IP-capable interconnecting network, the Transit Function forwards the SIP INVITE to the exit IBCF. The exit IBCF sends an HTTP POST containing two signing requests to the STI-AS, one to request signing of the caller identity and one to request signing of the RPH and SIP Priority header. The STI-AS signs the caller identity and the RPH/SIP Priority header and returns identityHeader parameters associated with the caller identity and the RPH/SIP Priority header to the exit IBCF in an HTTP 200 OK message that contains two signing responses. The exit IBCF then forwards the call via the NNI to an entry IBCF in the interconnecting network. This example assumes that the exit IBCF forwards the SIP INVITE to the entry IBCF in the emergency caller's home network. Depending on the scenario, the callback call may traverse other interconnecting networks before reaching the emergency caller's home network.

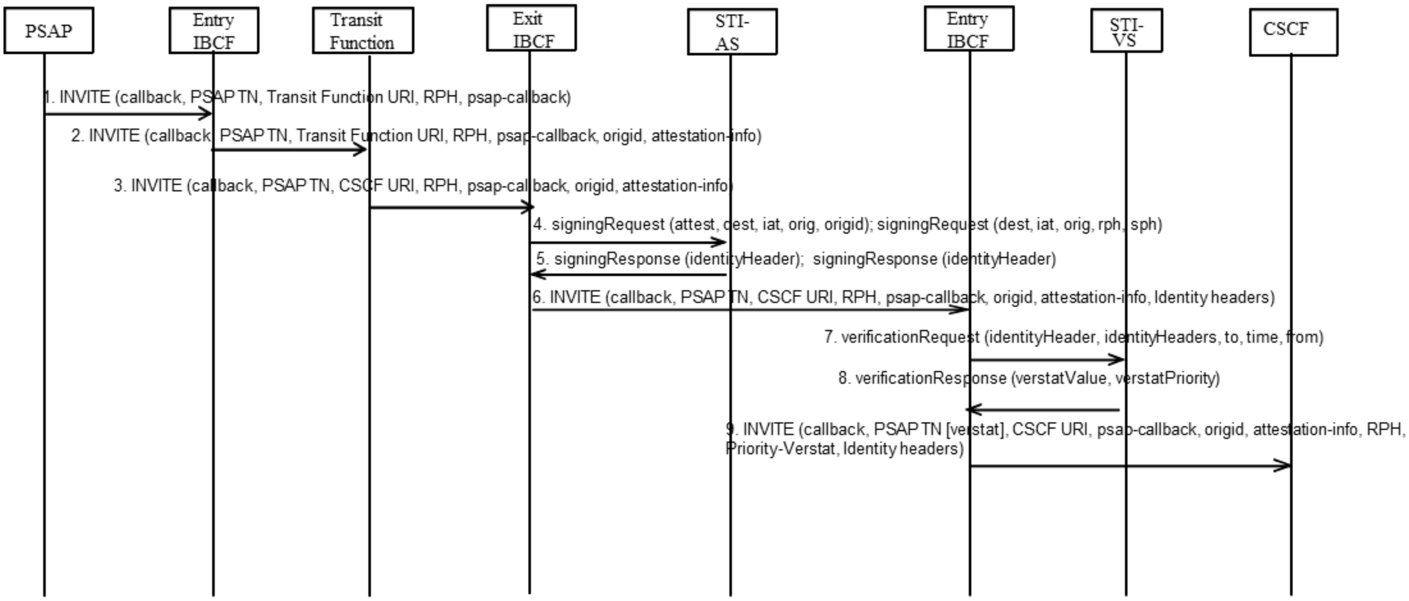

PSAP
Entry IBCF
Transit Function
Exit IBCF
STI-AS
Entry IBCF
STI-VS
CSCF
1. INVITE (callback, PSAP TN, Transit Function URI, RPH, psap-callback)
2. INVITE (callback, PSAP TN, Transit Function URI, RPH, psap-callback, origid, attestation-info)
3. INVITE (callback, PSAP TN, CSCF URI, RPH, psap-callback, origid, attestation-info)
4. signingRequest (attest, dest, iat, orig, origid); signingRequest (dest, iat, orig, rph, sph)
5. signingResponse (identityHeader); signingResponse (identityHeader)
6. INVITE (callback, PSAP TN, CSCF URI, RPH, psap-callback, origid, attestation-info, Identity headers)
7. verificationRequest (identityHeader, identityHeaders, to, time, from)
8. verificationResponse (verstatValue, verstatPriority)
9. INVITE (callback, PSAP TN [verstat], CSCF URI, psap-callback, origid, attestation-info, RPH, Priority-Verstat, Identity headers)

**Figure 8-47: Callback Call with Caller Identity and RPH Signing Initiated by Exit IBCF**

**Step 1.** The PSAP Call Handling Function initiates a callback call, generating a SIP INVITE message with the callback URI from the original emergency call in the To header and Request-URI, the TN of the PSAP originating the callback (i.e., sip:TN@<psapdomain>;user=phone) in the From and P-Asserted-Identity headers, "psap-callback" in the Priority header, and "esnet.0" in the Resource-Priority header. The PSAP Call Handling Function passes the SIP INVITE via a BCF (not shown) to an entry IBCF in an IMS-based NG9-1-1 Emergency Services Network.

**Step 2.** Upon receiving the SIP INVITE message, the entry IBCF applies general screening rules to the request and, based on local policy, adds an Origination-Id header to the INVITE to indicate from where the request was received, as well as an Attestation-Info header indicating the attestation level associated with the PSAP telephone number. It then forwards the INVITE to the Transit Function.

**Step 3.** The Transit Function uses the destination address (i.e., the callback URI) in the Request-URI to determine the routing for the call. The Transit Function determines that the call is to be routed to an interconnecting IP network, and forwards the SIP INVITE message to the exit IBCF.

**Step 4.** The exit IBCF sends an HTTP POST message containing two signing requests over the Ms reference point to the STI-AS. The signingRequest associated with the caller identity includes an "attest" parameter and an "origid" parameter, populated according to local policy or based on information received by the IBCF in an Attestation-Info header and an Origination-Id header, respectively, within the SIP INVITE. The signingRequest also includes other PASSporT information (i.e., "orig", "dest", and "iat"). The signingRequest associated with the RPH/Priority header will include an "rph" claim that contains an assertion value of "esnet.0", along with the "orig", "dest", and "iat", and an "sph" claim with a value of "psap-callback". The exit IBCF determines the assertion value for the "rph" and "sph" claims based on the RPH and Priority header received in the SIP INVITE message.

**Step 5.** The STI-AS determines through service provider-specific means the legitimacy of the content of the caller identity and the RPH information in the signing requests. The STI-AS then securely requests its private key from the SKS (not shown). The STI-AS uses the key to sign and populate identityHeader parameters associated with the caller identity and RPH/SIP Priority header in signing responses within the HTTP 200 OK message that it returns to the exit IBCF.

**Step 6.** In this example, the exit IBCF forwards the SIP INVITE to the entry IBCF in the emergency caller's home network. It uses the identityHeader parameters received in the signing responses to populate Identity headers in the outgoing SIP INVITE message. If, based on local policy, a verstat is present in the received SIP INVITE, the exit BCF will remove the verstat before forwarding the call to the next network.

**Step 7.** The entry IBCF in the emergency caller's home network initiates an HTTP POST message to the STI-VS that includes a verificationRequest containing an "identityHeader" claim corresponding to the Identity header containing signed caller identity information, an "identityHeaders" claim corresponding to the Identity header containing the signed RPH and Priority header information, as well as a "to" parameter containing the destination identity from the To header, a "from" parameter containing the asserted identity from the From or P-Asserted-Identity, and a "time" parameter based on the Date header field in the incoming request.

**Step 8.** The STI-VS determines the STI-CR Uniform Resource Identifier (URI) and makes an HTTPS request to the STI-CR (not shown). The STI-VS validates the certificate and then extracts the public key. It uses the public key to verify the signature in the identityHeader parameter, which validates the caller identity and the signature in the identityHeaders parameter which validates the RPH and SIP Priority header content signed by the IMS-based NG9-1-1 Emergency Services Network STI-AS. The STI-VS may interact with the CVT based on local policy and agreements between the home network provider and the analytics/CVT provider. The STI-VS returns an HTTP 200 OK containing a verificationResponse to the ingress IBCF. The verificationResponse contains a "verstatValue" parameter (associated with the "identityHeader" parameter in the verificationRequest) and a "verstatPriority" parameter (associated with the "identityHeaders" parameter in the verificationRequest) that indicates the result of the verification process. Depending on the results of the verification process, the "verstatValue" associated with the signed caller identity will be set to "TN-Validation-Passed", "TN-Validation-Failed", or "No-TN-Validation", and the "verstatPriority" associated with the signed RPH/SIP Priority header will be set to "ECB-RPH-Validation-Passed", "ECB-RPH-Validation-Failed", or "No-ECB-RPH-Validation".

**Step 9.** The entry IBCF continues to set up the callback call to the CSCF. The SIP INVITE message includes the callback number associated with the emergency caller, the PSAP telephone number and associated verstat parameter, the URI of the target CSCF, the RPH set to "esnet.0", a Priority header set to "psap-callback", a Priority-Verstat header field containing verification status information associated with the RPH/SIP Priority header, the Origination-Id, the Attestation-Info header, and the Identity headers.

### 8.12.5 Callback to Non-IMS VoIP Home Network – Transit Function Interacts with STI-AS

In this call flow example, an i3 PSAP initiates a callback call by sending a SIP INVITE that includes a To header and Request-URI that contains the callback number from the original emergency call, From and P-Asserted-Identity headers that contain the telephone number of the PSAP, "psap-callback" in the Priority header, and "esnet.0" in the Resource-Priority header, via a BCF (not pictured) to an entry IBCF in the IMS-based NG9-1-1 Emergency Services Network. The entry IBCF performs normal screening and based on local policy, adds an Origination-Id header to the INVITE to indicate from where the request was received, as well as an Attestation-Info header. The IBCF then passes the SIP INVITE to the Transit Function. In this call flow example, after determining that the call is to be directed to an IP-capable interconnecting network, the Transit Function forwards the SIP INVITE to the STI-AS. The STI-AS performs attestation and authentication of the caller identity information and signing of the RPH and SIP Priority header, then populates an Identity header associated with the caller identity and an Identity header associated with the signed RPH/SIP Priority header in the SIP INVITE and returns it to the Transit Function. The Transit Function then routes the callback call to an egress IBCF in the IMS-based NG9-1-1 Emergency Services Network which forwards the call via the NNI to a VoIP Service Provider (VSP) Call Server/Proxy in the emergency caller's home network. Depending on the scenario, the callback call may traverse other interconnecting networks before reaching the emergency caller's home network.

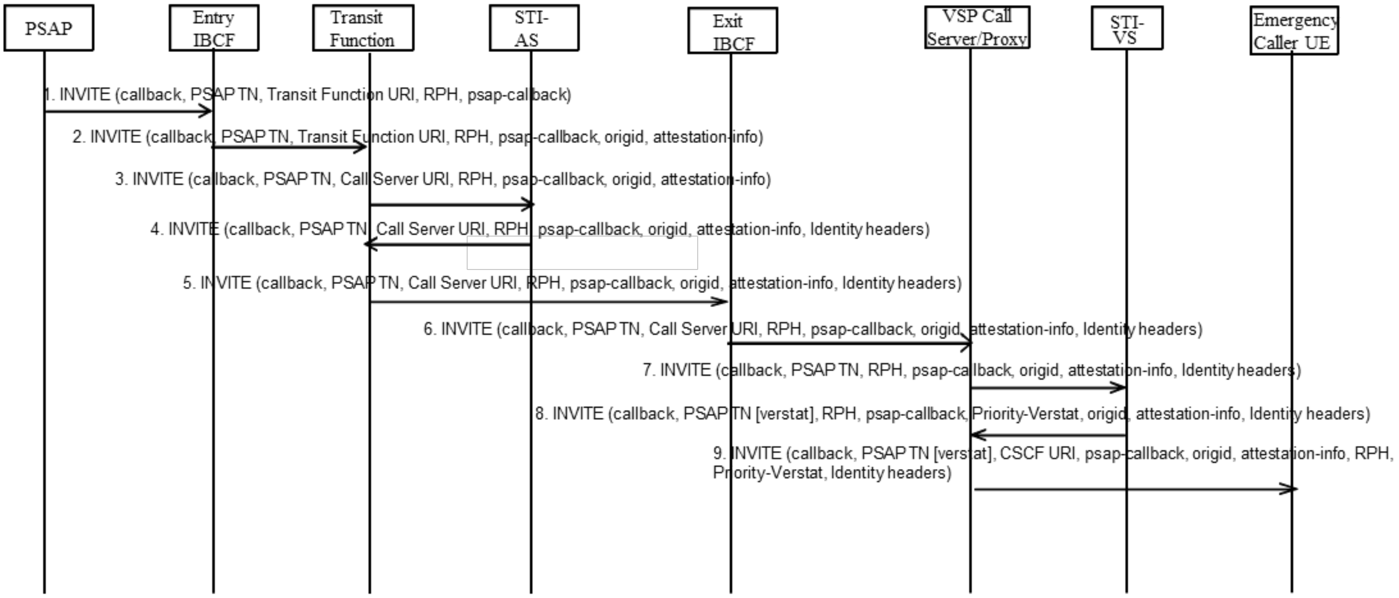

PSAP
Entry IBCF
Transit Function
STI-AS
Exit IBCF
VSP Call Server/Proxy
STI-VS
Emergency Caller UE
1. INVITE (callback, PSAP TN, Transit Function URI, RPH, psap-callback)
2. INVITE (callback, PSAP TN, Transit Function URI, RPH, psap-callback, origid, attestation-info)
3. INVITE (callback, PSAP TN, Call Server URI, RPH, psap-callback, origid, attestation-info)
4. INVITE (callback, PSAP TN, Call Server URI, RPH, psap-callback, origid, attestation-info, Identity headers)
5. INVITE (callback, PSAP TN, Call Server URI, RPH, psap-callback, origid, attestation-info, Identity headers)
6. INVITE (callback, PSAP TN, Call Server URI, RPH, psap-callback, origid, attestation-info, Identity headers)
7. INVITE (callback, PSAP TN, RPH, psap-callback, origid, attestation-info, Identity headers)
8. INVITE (callback, PSAP TN [verstat], RPH, psap-callback, Priority-Verstat, origid, attestation-info, Identity headers)
9. INVITE (callback, PSAP TN [verstat], CSCF URI, psap-callback, origid, attestation-info, RPH, Priority-Verstat, Identity headers)

**Figure 8-48: Callback Call to VoIP Home Network with Caller Identity and RPH Signing Initiated by Transit Function**

**Step 1.** The PSAP Call Handling Function initiates a callback call, generating a SIP INVITE message with the callback URI from the original emergency call in the To header and Request-URI, the TN of the PSAP originating the callback (i.e., sip:TN@<psapdomain>;user=phone) in the From and P-Asserted-Identity headers, “psap-callback” in the Priority header, and “esnet.0” in the Resource-Priority header. The PSAP Call Handling Function passes the SIP INVITE via a BCF (not shown) to an entry IBCF in an IMS-based NG9-1-1 Emergency Services Network.

**Step 2.** Upon receiving the SIP INVITE message, the entry IBCF applies general screening rules to the request and, based on local policy, adds an Attestation-Info header and an Origination-Id header (to indicate from where the request was received) to the INVITE. It then forwards the INVITE to the Transit Function.

**Step 3.** The Transit Function uses the destination address (i.e., the callback URI) in the Request-URI to determine the routing for the call. Before forwarding the call to the interconnecting network, the Transit Function sends the request to the STI-AS for authentication and signing of the caller identity and signing of the RPH and SIP Priority header.

**Step 4.** The STI-AS determines, through service provider-specific means, the legitimacy of the content of the caller identity and the RPH and SIP Priority header fields. The STI-AS then securely requests its private key from the SKS (not shown). Upon receiving the private key from the SKS, the STI-AS signs the caller identity and RPH/SIP Priority header and adds Identity header fields (one associated with the caller identity and one associated with the RPH/SIP Priority header) to the SIP INVITE message. The STI-AS then returns the SIP INVITE, with the signed Identity headers, to the Transit Function.

**Step 5.** The Transit Function routes the SIP INVITE (with the Identity headers) to the exit IBCF.

**Step 6.** In this example, the exit IBCF forwards the SIP INVITE to a VSP Call Server/Proxy (via a BCF/SBC [not shown]) in the emergency caller’s home network. If, based on local policy, a verstat is present in the SIP INVITE received by the IBCF, the IBCF will remove the verstat before forwarding the call to the next network. Note that depending on the scenario, the callback call may traverse other interconnecting networks before reaching the emergency caller’s home network.

**Step 7.** The VSP Call Server/Proxy in the emergency caller’s home network forwards the SIP INVITE message containing the Identity headers to the STI-VS.

**Step 8.** The STI-VS determines the STI-CR Uniform Resource Identifier (URI) and makes an HTTPS request to the STI-CR (not shown). The STI-VS validates the certificate and then extracts the public key. It uses the public key to verify the signature in the Identity headers, which validate the caller identity and the RPH and SIP Priority header content signed by the IMS-based NG9-1-1 Emergency Services Network STI-AS. The STI-VS may interact with the CVT based on local policy and agreements between the home network provider and the analytics/CVT provider. The STI-VS returns the SIP INVITE message to the VSP Call Server/Proxy. The SIP INVITE message includes verstat information associated with the caller identity as a parameter in the P-Asserted-Identity header and verification status information associated with the RPH/SIP Priority header in a Priority-Verstat header field, indicating the result of the verification process.

**Step 9.** The VSP Call Server/Proxy continues to set up the callback call to the emergency caller's UE. The SIP INVITE message includes the callback number associated with the emergency caller, the PSAP telephone number and associated verstat parameter, the RPH set to "esnet.0", a Priority header set to "psap-callback", a Priority-Verstat header field containing verification status information associated with the RPH/SIP Priority header, an Origination-Id header, an Attestation-Info header, and the Identity headers.

### 8.12.6 Callback to Non-IMS VoIP Home Network – Exit IBCF Interacts with STI-AS

In this call flow example, an i3 PSAP initiates a callback call by sending a SIP INVITE that includes a To header and Request-URI that contains the callback number from the original emergency call, From and P-Asserted-Identity headers that contain the telephone number of the PSAP, "psap-callback" in the Priority header, and "esnet.0" in the Resource-Priority header, via a BCF (not pictured) to an entry IBCF in the IMS-based NG9-1-1 Emergency Services Network. The entry IBCF performs normal screening and based on local policy, adds an Origination-Id header to the INVITE to indicate from where the request was received, as well as an Attestation-Info header. The IBCF then passes the SIP INVITE to the Transit Function. In this call flow example, after determining that the call is to be directed to an IP-capable interconnecting network, the Transit Function forwards the SIP INVITE to the exit IBCF. The exit IBCF sends an HTTP POST message containing two signing requests to the STI-AS, one requesting signing of the caller identity and the other requesting signing of the RPH and SIP Priority header content. The STI-AS signs the caller identity and the RPH/SIP Priority header and returns identityHeader parameters associated with the caller identity and the RPH/SIP Priority header to the exit IBCF in an HTTP 200 OK message containing two signing responses. The exit IBCF then forwards the call via the NNI to an entry IBCF/BCF in the interconnecting network. This example assumes that the exit IBCF forwards the SIP INVITE to a VSP Call Server/Proxy (via a BCF/SBC [not shown]) in the emergency caller's home network. Depending on the scenario, the callback call may traverse other interconnecting networks before reaching the emergency caller's home network.

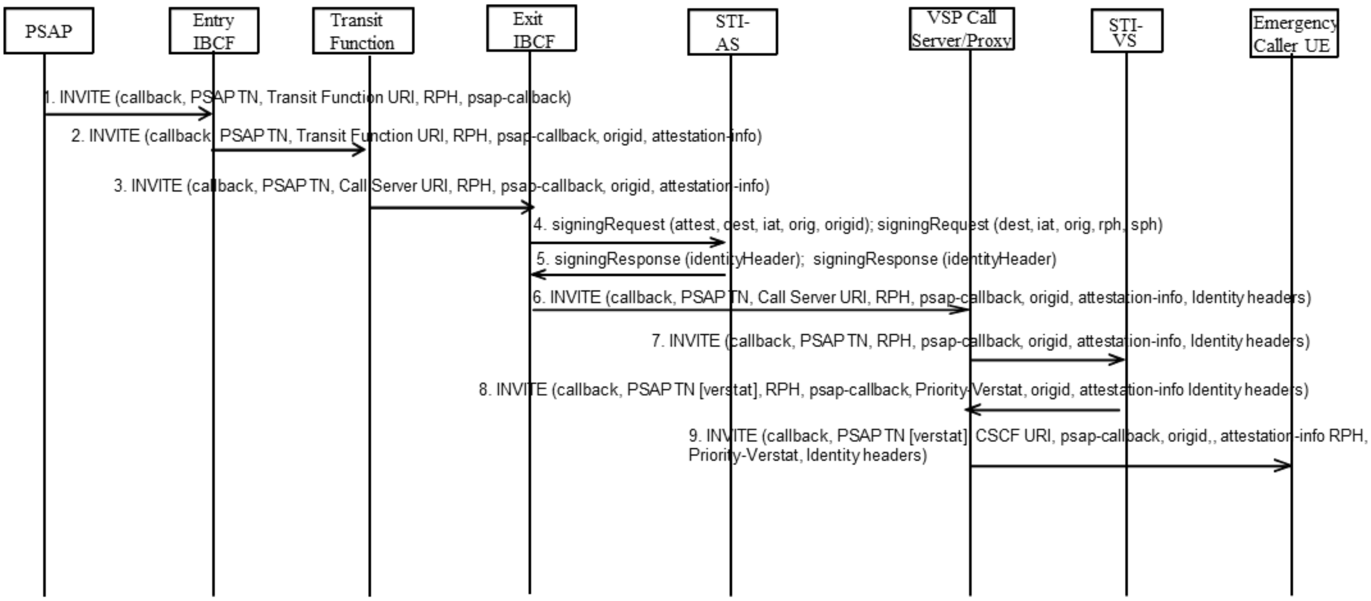

PSAP
Entry IBCF
Transit Function
Exit IBCF
STI-AS
VSP Call Server/Proxy
STI-VS
Emergency Caller UE
1. INVITE (callback, PSAP TN, Transit Function URI, RPH, psap-callback)
2. INVITE (callback, PSAP TN, Transit Function URI, RPH, psap-callback, origid, attestation-info)
3. INVITE (callback, PSAP TN, Call Server URI, RPH, psap-callback, origid, attestation-info)
4. signingRequest (attest, dest, iat, orig, origid); signingRequest (dest, iat, orig, rph, sph)
5. signingResponse (identityHeader); signingResponse (identityHeader)
6. INVITE (callback, PSAP TN, Call Server URI, RPH, psap-callback, origid, attestation-info, Identity headers)
7. INVITE (callback, PSAP TN, RPH, psap-callback, origid, attestation-info, Identity headers)
8. INVITE (callback, PSAP TN [verstat], RPH, psap-callback, Priority-Verstat, origid, attestation-info Identity headers)
9. INVITE (callback, PSAP TN [verstat], CSCF URI, psap-callback, origid,, attestation-info RPH, Priority-Verstat, Identity headers)

**Figure 8-49: Callback Call to VoIP Home Network with Caller Identity and RPH Signing Initiated by Exit IBCF**

**Step 1.** The PSAP Call Handling Function initiates a callback call, generating a SIP INVITE message with the callback URI from the original emergency call in the To header and Request-URI, the TN of the PSAP originating the callback (i.e., sip:TN@<psapdomain>;user=phone) in the From and P-Asserted-Identity headers, "psap-callback" in the Priority header, and "esnet.0" in the Resource-Priority header. The PSAP Call Handling Function passes the SIP INVITE via a BCF (not shown) to an entry IBCF in an IMS-based NG9-1-1 Emergency Services Network.

**Step 2.** Upon receiving the SIP INVITE message, the entry IBCF applies general screening rules to the request and, based on local policy, adds an Origination-Id header to the INVITE to indicate from where the request was received, as well as an Attestation-Info header indicating the attestation level associated with the PSAP telephone number. It then forwards the INVITE to the Transit Function.

**Step 3.** The Transit Function uses the destination address (i.e., the callback URI) in the Request-URI to determine the routing for the call. The Transit Function determines that the call is to be routed to an interconnecting IP network, and forwards the SIP INVITE message to the exit IBCF.

**Step 4.** The exit IBCF sends an HTTP POST containing two signing requests over the Ms reference point to the STI-AS. The signingRequest associated with the caller identity includes an "attest" parameter and an "origid" parameter, populated according to local policy or based on information received by the IBCF in an Attestation-Info header and an Origination-Id header, respectively, within the SIP INVITE. The signingRequest also includes other PASSporT information (i.e., "orig", "dest", and iat). The second signingRequest includes an "rph" claim that contains an assertion value of "esnet.0", and an "sph" claim with a value of "psap-callback", as well as a "dest", "orig", and "iat". This call flow assumes that the exit IBCF populates the assertion values in the "rph" and "sph" claims based on the RPH and SIP Priority header fields received in the SIP INVITE message .

**Step 5.** The STI-AS determines through service provider-specific means the legitimacy of the content of the caller identity and the RPH and SIP Priority header information in the signing requests. The STI-AS then securely requests its private key from the SKS (not shown). The STI-AS uses the key to sign and populate identityHeader parameters associated with the caller identity and RPH/SIP Priority header in the two signing responses that it returns to the exit IBCF in an HTTP 200 OK message.

**Step 6.** In this example, the exit IBCF forwards the SIP INVITE to a VSP Caller Server/Proxy in the emergency caller's home network (via a BCF/SBC [not shown]). It uses the identityHeader parameters received in the signing responses to populate Identity headers in the outgoing SIP INVITE message. If, based on local policy, a verstat is present in the received SIP INVITE, the exit BCF will remove the verstat before forwarding the call to the next network.

**Step 7.** The VSP Call Server/Proxy in the emergency caller's home network forwards the SIP INVITE message containing the Identity headers to the STI-VS.

**Step 8.** The STI-VS determines the STI-CR Uniform Resource Identifier (URI) and makes an HTTPS request to the STI-CR (not shown). The STI-VS validates the certificate and then extracts the public key. It uses the public key to verify the signature in the Identity headers, which validate the caller identity and the RPH and SIP Priority header content signed by the IMS-based NG9-1-1 Emergency Services Network STI-AS. The STI-VS may interact with the CVT based on local policy and agreements between the home network provider and the analytics/CVT provider. The STI-VS returns the SIP INVITE message to the VSP Call Server/Proxy. The SIP INVITE message includes verstat information associated with the caller identity as a parameter in the P-Asserted-Identity header and the verification status information associated with the RPH/SIP Priority header in a Priority-Verstat header field, indicating the results of the verification process.

**Step 9.** The VSP Call Server/Proxy continues to set up the callback call to the emergency caller's UE. The SIP INVITE message includes the callback number associated with the emergency caller, the PSAP telephone number and associated verstat parameter, the RPH set to "esnet.0", a Priority header set to "psap-callback", a Priority-Verstat header field containing verification status information associated with the RPH/SIP Priority header, an Origination-Id header, an Attestation-Info header and the Identity headers.

# 9 Stage 3

This clause defines stage 3 procedures for the network elements within an IMS-based NG9-1-1 Emergency Services Network. This clause refers to 3GPP TS 24.229 [Ref 2] and illustrates the use within an emergency services network. This clause also illustrates header usage and examples.

## *9.1 Procedures & Header Usage for the Emergency CSCF (E-CSCF)*

For North America, the E-CSCF shall follow the procedures in Clauses 4 and 5.11.1 General of 3GPP TS 24.229 [Ref 2] with the following clarifications:

1. The E-CSCF receives all SIP requests from the I-CSCF. The P-CSCF is not applicable in this architecture.
2. The E-CSCF shall always query the LRF for routing instructions (i.e., the PSAP URI) and, potentially, user device location.
3. The E-CSCF connects to NENA i3 PSAPs via an (egress) IBCF. The E-CSCF connects to legacy PSAPs via an IBCF and an LPG.
4. Emergency dialogs requesting privacy as noted in 3GPP TS 22.101 [Ref 3] shall not be supported in North America.

Due to the placement of the E-CSCF in the IMS-based NG9-1-1 Emergency Services Network, not all of the procedures contained in Clause 5.11.2 of 3GPP TS 24.229 [Ref 2] (UE originating case) are applicable. Only the following procedures apply with the clarifications provided below:

1. (5.11.2 step 1A) The E-CSCF will remove its own SIP URI from the topmost Route header field.
2. (5.11.2 step 1D) Since an LRF is to be used, the E-CSCF will forward the request to the LRF as defined in subclause 5.11.3 of 3GPP TS 24.229 [Ref 2]. It will pass all headers received from the I-CSCF.

3. When the 300 response is received (as described in Clause 5.11.3 of 3GPP TS 24.229 [Ref 2]), the E-CSCF will map Contact header parameters as specified below.
4. For North America, the E-CSCF will forward a SIP INVITE destined for an i3 PSAP or a legacy PSAP via an IBCF based on the Route URI received in the Contact header of the 300 Multiple Choices message received from the LRF, as described below.
5. An E-CSCF operating in an emergency services network in North America may, as an implementation option, create a Record-Route header field containing its own SIP URI.

   NOTE: Operators may wish to consider whether the optional SUBSCRIBE/NOTIFY mechanism between the E-CSCF and the LRF will be implemented, as well as the transfer mechanism supported, in determining whether an E-CSCF operating in their emergency services network creates a Record-Route header field containing its own SIP URI.
6. (5.11.2 step 10) If the request is an INVITE request, the E-CSCF shall save Contact, CSeq, and Record-Route header field values received in the request such that the E-CSCF is able to release the session if needed.
7. (5.11.2 step 13) The E-CSCF shall route the request based on SIP routing procedures.

The E-CSCF shall not create the P-Charging-Vector or P-Charging-Address headers, but pass any received in the incoming SIP INVITE. If the P-Charging-Vector header is included in the incoming SIP INVITE it is expected that it identifies the carrier.

For North America, the E-CSCF shall follow the procedures in 3GPP TS 24.229 [Ref 2] Clause 5.11.3, *Use of LRF*, with the following clarifications:

- The E-CSCF shall route to the LRF the initial request for a dialog containing an emergency service URN that it received from the I-CSCF. The Request URI of urn:service:sos will be received from the I-CSCF and will not be modified by the E-CSCF.
- The E-CSCF will not insert a P-Charging-Vector header field.
- When the E-CSCF receives any 3xx response to such a request, the E-CSCF shall select a Contact header and parse it as described below, and will follow the procedures above and not those in Clause 5.11.2 of 3GPP TS 24.229 [Ref 2].
- The E-CSCF shall also follow the procedures adopted in Clause 5.11.3 of 3GPP TS 24.229 [Ref 2] with the following clarifications:
  - When the E-CSCF receives a SIP 300 Multiple Choices message from an LRF that contains a Contact URI parameter of “Route”, it shall populate the outgoing SIP INVITE as shown in Clause 9.1.1.
  - As described in Clause 5.11.3 of 3GPP TS 24.229 [Ref 2], if the E-CSCF does not receive a SIP 300 Multiple Choices in response to a request sent to the LRF within an operator settable timeout, the E-CSCF shall use a default URI value (configured in the E-CSCF) in the Route header of the outgoing SIP INVITE message.
- The E-CSCF shall pass the following header fields associated with caller identity authentication and RPH and SIP Priority header signing/verification forward, unchanged, if received in a SIP INVITE message: one or more Identity header fields; a Priority-Verstat header field; an Attestation-Info header; an Origination-Id header.

### 9.1.1 Header Usage

This clause denotes specific use of headers in this standard in compliance with the respective RFCs. Only pertinent headers are discussed. Any SIP headers received from the I-CSCF not modified in this clause should be passed unmodified.

**Parsing of the 300 Multiple Choices Contact Header**

The Contact header in the 300 Multiple Choices response shall contain the Route URI that designates either a legacy or NENA i3 PSAP.

***Request Line***

On an outgoing initial SIP INVITE toward a legacy PSAP or a NENA i3 PSAP, the E-CSCF shall copy the emergency services URN received in the Request URI of the incoming SIP INVITE to the Request URI header of the outgoing SIP INVITE message.

Example:

```
INVITE urn:service:sos SIP/2.0
```

***Route***

The Route parameter is returned in the 300 Multiple Choices response to allow the E-CSCF to determine how to route the call. The Route parameter will contain a sip URI (e.g., sip: `psap@st.county.net`).

The E-CSCF will use the Route parameter to create a Route header in the outgoing SIP INVITE and will populate the Route header with the sip URI that was provided in the Route parameter.

Example:

```
Route:sip:psap@st.county.net
```

## *9.2 Procedures & Header Usage for the Location Retrieval Function (LRF)*

The LRF procedures are defined in 3GPP TS 24.229 [Ref 2] Clauses 4, 5.11.3, and 5.12. For North America, the following clarifications apply:

### 9.2.1 Processing of Origination from i3-Compliant Originating Network or LNG

Emergency originations from i3-compliant originating networks or LNGs are expected to include a Geolocation header. When a Geolocation header is present in the SIP INVITE message received from the E-CSCF, then the following conditions apply:

- If the Geolocation header contains a “cid” that defines that the location is in the body of the request (i.e., LbyV), the LRF will use that location in subsequent processing.
- If the Geolocation header contains a location reference URI (i.e., LbyR), the LRF will retrieve the location via the D1 Reference Point and will use that location in subsequent processing.

Having obtained location information for the emergency call, the LRF uses that location information to query the RDF for routing information.

If a Geolocation header is not present in the SIP INVITE message received from the E-CSCF, then the LRF will return a configured default Route URI to the E-CSCF in the 300 Multiple Choices response.

### 9.2.2 Using Incoming Signaling Information to Facilitate Error Handling

To facilitate error processing for calls that entered the IMS-based NG9-1-1 Emergency Services Network via an LNG, the LRF may use the trunk group (tgrp) and trunk group context parameters that may have been populated by the LNG in the Contact header of the outgoing SIP INVITE message. If the tgrp and trunk-context parameters are included in the incoming Contact header, and the LRF contains pre-provisioned error handling rules, the LRF may use those rules to provide routing instructions back to the E-CSCF. This allows the LRF to provide different error handling based upon the class of service associated with the SS7 trunk group. Alternatively, the LRF can use class of service information available in the Additional Data provided in the incoming SIP INVITE message as a basis for error handling.

### 9.2.3 Header Usage

This clause discusses headers used in the SIP 300 Multiple Choices response to the E-CSCF.

**Contact Header**

The Contact header in the 300 Multiple Choices message from the LRF will contain the Route URI provided by the RDF. The E-CSCF will use this Route header to forward the emergency call request toward the PSAP.

**Example:**

The following example illustrates the Contact header for an emergency call request being routed to a NENA i3 PSAP. (BCF headers are not accounted for.)

```
Contact:<sip:psap.st.county.net;lr>
```

The following example illustrates the Contact header for an emergency call request being routed to a legacy PSAP via the LPG. (BCF headers are not accounted for.)

```
Contact:<sip:psap.st.county.LPG.provider.example.net;lr>
```

### 9.2.4 Procedures at Policy Routing Function (PRF)

The PRF is a functional component of the LRF. As such, this standard only defines the functionality associated with a PRF and does not specify the interfaces or define new reference points between the LRF and the PRF.

The PRF determines whether an alternate PSAP should be chosen based upon pre-defined policy routing rules. For example, policy routing rules may be associated with night closure of a PSAP, scheduled maintenance, or other events/conditions that may prevent the PSAP from receiving emergency call requests. The policy routing rules governing these conditions/events, and the identification of the alternate PSAP, are specified by the PSAP or the 9-1-1 Authority.

After the LRF receives routing instructions (i.e., a Route URI) from the RDF, it interrogates the PRF with this Route URI to determine if there are policy routing rules that should modify the routing instructions that will be returned to the E-CSCF by the LRF. The PRF interrogates its internal policy store with this URI. In evaluating the rule set(s) for this URI the PRF may consider other inputs available to it, such as header fields in the received SIP INVITE message, time of day, PSAP state, etc.  If dictated by policy, the PRF may obtain an alternate URI. This URI will be returned to the LRF, which in turn, will use this URI rather than the one that the LRF received from the RDF as the "next hop" URI.

### 9.2.4.1 Route Policy Syntax

This clause describes the syntax and semantics of the policy language used for making policy-based call routing decisions. A policy document is a JSON Web Signature (JWS); the payload is a JSON object conformant to Appendix E.1 of NENA-STA-010.3 [Ref 27]. Policies stored in the Policy Store must be signed by the owner of the policy. A policy document is composed of a set of rules, and an optional description. Each rule is a JSON object containing the following members: "id" (required), "priority" (required), "conditions" (optional), "actions" (required), and "description" (optional). Within a rule, the "conditions" object evaluates to 'true' or 'false'. If it evaluates to 'true', then the "actions" portion of the rule is eligible to be executed. Because multiple rules might have "condition" objects that evaluate to 'true', each rule has an associated priority value. A rule with a higher (numerically greater) value takes precedence over a rule with a lower value. When more than one rule has a "conditions" object that evaluates to 'true', only the rule with the largest priority value has its "actions" executed. Priority 0 is the lowest priority; a rule with priority 0 is only executed if no other rule's "conditions" evaluate to 'true'. Each rule also has an ID, which is a string unique to the ruleset. The LRF must verify the JWS signature before executing the rules. The Policy Store is required to support the storage and retrieval of Route Policy documents byte-for-byte unaltered (so that the JWS extracted is the exact same octet stream stored, and calculates the exact same digest). (See Clause 9.2.4.2 for further discussion of the Policy Store Web Service.) If the JWS signature verification fails, the policy must not be executed. An LRF that detects a failed JWS signature verification should file a Policy Discrepancy Report (as described in Clause 3.7.13 of NENA-STA-010.3 [Ref 27]) against the policy owner, and may file a Policy Store Discrepancy Report (as described in Clause 3.7.4 of NENA-STA-010.3 [Ref 27]) against the Policy Store.

Examples of conditions that may be considered by the PRF include:

- Time period
- SIP header
- Additional Data
- Location (per RFC 6772 [Ref 61])
- Request URI
- LoST Service URN
- Queue State
- Service State
- Call Source (i.e., the originating network as defined by the Via header fields of the INVITE)
- Body element (i.e., any element contained within a message body or body part)
- Normal Next Hop (i.e., the URI retrieved from the LoST query)
- SDP Offer (to support the construction of a rule to route based on media as well as human interactive language associated with a type of media as indicated in the SDP)
- Calling Number Verification Status (allows testing of outcome of any validation of the calling number that may have been done by the STI-VS).

See Clause 3.3.3 of NENA-STA-010.3 [Ref 27] for further details.

### 9.2.4.2 Policy Store Web Service

Policies are stored into and retrieved from a Policy Store using a web service. Policies are named for the function that the policy affects (e.g., a RoutePolicy may be invoked by an LRF that is determining the Route URI to be returned to the E-CSCF). A policy consists of a set of rules and is sometimes referred to as a "ruleset". A specific Policy ruleset is uniquely identified by the combination of the policy name and the ID of the agency that owns (created) the policy. A Policy Store accepts a policy document from a policy owner and provides it on request to a policy retriever via a web service. Policies stored in the Policy Store must be signed by the owner of the policy.

The web service supports the following functions:

- StorePolicy: This function initiates the creation of a policy ruleset in the Policy Store. The StorePolicy function uses a POST operation with a request body that contains the Policy as a JWS. Upon receiving the POST, the Policy Store will confirm that: the policyExpirationTime is in the future; the size of the received policy exactly matches the size specified in policySize; the structure and content of the document is well-formed and conformant; and each Policy Routing rule has a unique ID. In addition, the Policy Store will verify the JWS signature.

- RetrievePolicy: This function uses a GET operation to retrieve a policy ruleset from the Policy Store. This function's parameters include at least one of the policy type, the identity of the policy owner, or the policy ID, and may include the maximum number of results that the retriever can receive at one time. The response will consist of an array of policy objects, each a JWS, as well as an indication of the number of items in the array and the total number of items found. The policy(ies) retrieved is(are) valid until the expiration time. If the policy is needed for use after expiration, it must be retrieved again from the Policy Store. Instead of returning the policy requested, the response may return a referral to another Policy Store that might have the policy via an HTTP 307 Temporary Redirect.

- DeletePolicy: This function deletes a policy set in the Policy Store. The parameters are the name of the policy and the agency whose policy is being deleted. For Policy Routing Rules, the delete request will also contain the ID.

- EnumeratePolicy: This function uses a GET operation to return a list of policy names available in the store for a specific agency. The parameters of the request are the policy type, policy owner, and/or policy ID, and optionally, the maximum number of policies to return and an indication of the timeframe in which the desired policies were created. The response includes an array of policies, each consisting of policy type, policy owner, policy ID (if a Policy Routing policy), the policy expiration time and the date/time of last modification. The response will also include a count of the number of items in the array and the number of items found. The enumeration includes only those policies that are actually stored in this specific instance of the Policy Store.

- UpdatePolicy: This function uses a PUT operation to initiate the update of a policy ruleset in the Policy Store. This function's parameters include the name of the policy, the agency or service whose policy is being updated, and for Policy Routing Rules, the ID. The request body contains the replacement policy as a JWS object. When processing an Update request, the Policy Store must confirm that the policy expiration time is in the future, the size of the received policy exactly matches the size specified in policy size, and that the structure and contents of the document is well-formed and conformant.  For Policy Routing Rules the Policy Store must also confirm that each file has a unique ID.  The Policy Store must verify the JWS signature.

See Clause 3.3.1.2 of NENA-STA-010.3 [Ref 27] for further details.

## *9.3 Procedures at the RDF*

The RDF will receive a location and service URN from the LRF, and return a Route URI that may be used to route the call to either the legacy PSAP or a NENA i3 PSAP. In either case, the RDF shall return a sip URI without “user=phone”.

If the RDF is unable to determine a Route URI based on the location provided in the routing request from the LRF, it should return a default Route URI to the LRF.

### 9.3.1 Procedures for Provisioning the RDF

The RDF is expected to store Geospatial data from a Geographic Information System (GIS) to support the routing of emergency calls. The provisioning of data into the RDF is expected to use a standardized interface from a GIS that contains an authoritative copy of GIS data.  This interface is referred to in this document as a “Spatial Interface” (SI).

The SI could be built into a GIS system, or could be a stand-alone element with proprietary interfaces to GIS systems and the standardized interface toward the data consumers. An SI provides an interface between an authoritative copy of GIS data and functional elements within an NG9-1-1 Emergency Services Network such as an RDF.

The SI interface is near-real-time; an authorized change to the authoritative GIS will be reflected in the RDF nearly immediately via the SI.

The data model for the SI is defined in Appendix B of NENA-STA-010.3 [Ref 27]. While the GIS Data Model, as described in NENA-STA-006.1-2018 [Ref 64], supports geospatial routing and location validation, the GIS data described in NENA-STA-006.1-2018 [Ref 64] need not be the same as that defined for the SI; the SI could transform internal GIS data to the SI structure.

The SI interface, as defined in NENA-STA-010.3 [Ref 27] is based on Open Geospatial Consortium (OGC) Document OGC 10-069r2 [Ref 54], which describes a layer replication interface service for geospatial databases using the OGC Web Feature Service 2.0 Interface Standard and the Atom protocol (see RFC 4287 [Ref 55] and RFC 5023 [Ref 56]). Changes in GIS data are expressed in Web Feature Service (WFS) Insert/Update/Delete actions and Atom is used to move the edits from the master (i.e., the authoritative GIS database) to the copy (i.e., the RDF database).

See Clause 3.6 of NENA-STA-010.3 [Ref 27] for further discussion.

## *9.4 Procedures at the LNG*

The LNG shall adhere to Clause 6.1 of NENA-STA-010.3 [Ref 27] with additions and clarifications noted in this Clause. The LNG will operate as an entry point for legacy emergency calls.

The LNG will map CAMA or Feature Group D (FG D) MF signaling, or SS7 parameters into SIP headers based upon the type of signaling on the incoming trunk group. The types of signaling supported are: SS7 wireline, CAMA wireline, FG D wireline, SS7 Wireline Compatibility Mode (WCM) for wireless, CAMA WCM for wireless, FG D for wireless, SS7 Non-Call Associated Signaling (NCAS), CAMA NCAS, and FG D NCAS.

Table 9-1 provides a summary of the signaling mappings that an entry LNG must be capable of performing to support emergency originations from legacy wireline and legacy wireless networks.

**Table 9-1: Mapping at LNG**

| | CdPN | CPN | CN/ANI | GDP | From | To | R-URI | PAI | P-Charge-Info |
|---|---|---|---|---|---|---|---|---|---|
| **Legacy Wireline – SS7** | 911 | TN | CN | - | TN | 911 | sos | TN | CN |
| **Legacy Wireline – MF** | 911 | - | ANI | - | ANI | 911 | sos | ANI | ANI |
| **Legacy Wireless – WCM-SS7** | 911 | ESRK | CN | - | CBN | 911 | sos | CBN | CN |
| **Legacy Wireless – WCM-MF** | 911 | - | ESRK | - | CBN | 911 | sos | CBN | ESRK |
| **Legacy Wireless – NCAS-SS7** | 911 | TN | CN | ESRD/K | TN | 911 | sos | TN | CN |
| **Legacy Wireless – NCAS-MF** | ESRD/K | - | ANI | - | ANI | 911 | sos | ANI | ANI |

Table 9-2 through Table 9-10 provide examples of the mappings that will be performed by an LNG from various types of incoming SS7 and MF signaling to SIP.

### 9.4.1 SS7 Wireline to SIP Header Mapping Example

Table 9-2 illustrates the mapping from SS7 parameters to the SIP headers sent to the I-CSCF in the outgoing SIP INVITE message for wireline calls. The Called Party Number (CdPN) and Calling Party Number (CPN) parameters are mapped as shown in the table.

**Table 9-2: SS7 Wireline to SIP Header Mapping Example**

| SS7 Parameter | SS7 Example | SIP Header | SIP Example |
|---|---|---|---|
| CPN | 3125551234 | From | <sip:+13125551234@carrier.example.net;user=phone> |
| CdPN | 911 | To | sip:911@carrier.example.com |
| CPN<br>OLI<br>CPC | 3125551234<br>00<br>emergency | PAI | <sip:+13125551234@carrier.example.net;user=phone> |
| NA | | Request URI | urn:service:sos |

### 9.4.2 CAMA Wireline to SIP Header Mapping Example

Table 9-3 illustrates the mapping from CAMA MF signaling to SIP headers sent to the I-CSCF in the outgoing SIP INVITE message for wireline calls. The Calling and Called Numbers are mapped as shown in the table. The NPA is populated by the LNG based on the incoming trunk group.

**Table 9-3: CAMA MF Wireline to SIP Header Mapping Example**

| CAMA Signaling | CAMA Example | SIP Header | SIP Example |
|---|---|---|---|
| Calling Number/ ANI | I+7digits<br>0+5551234 | From | <sip:+13125551234@carrier.example.net;user=phone> |
| Called Number | 911 | To | sip:911@carrier.example.com |
| Calling Number/ ANI | I+7digits<br>0+5551234 | PAI | <sip:+13125551234@carrier.example.net;user=phone> |
| NA | | Request URI | urn:service:sos |

### 9.4.3 FG D Wireline to SIP Header Mapping Example

Table 9-4 illustrates the mapping from FG D signaling to SIP headers sent to the I-CSCF in the outgoing SIP INVITE message for wireline calls. The Calling and Called Numbers are mapped as shown in the table.

**Table 9-4: FG D MF Wireline to SIP Header Mapping Example**

| FG D Signaling | CAMA Example | SIP Header | SIP Example |
|---|---|---|---|
| Calling Number | II+10-digits<br>00+ 3125551234 | From | <sip:+13125551234@carrier.example.net;user=phone> |
| Called Number | 911 | To | sip:911@carrier.example.com |
| Calling Number | II+10-digits<br>00+ 3125551234 | PAI | <sip:+13125551234@carrier.example.net;user=phone> |
| NA | | Request URI | urn:service:sos |

### 9.4.4 SS7 Wireline Compatibility Mode to SIP Header Mapping Example

Table 9-5 illustrates the mapping from SS7 parameters to SIP headers sent to the I-CSCF in the outgoing SIP INVITE message for Wireline Compatibility Mode (WCM) wireless calls. The Called Party Number is mapped as shown in the table. The content of the Calling Party Number parameter (i.e., the ESRK) is used to query the MPC/GMLC. The callback number received in the response from the MPC/GMLC is used to populate the From and PAI headers.

**Table 9-5: SS7 WCM to SIP Header Mapping Example**

| SS7 Parameter | SS7 Example | SIP Header | SIP Example |
|---|---|---|---|
| CPN (ESRK) | 7185111234 | From (CBN obtained from MPC/GMLC) | <sip:+13125551234@carrier.example.net;user=phone> |

| SS7 Parameter | SS7 Example | SIP Header | SIP Example |
|---|---|---|---|
| CdPN | 911 | To | sip:911@carrier.example.com |
| CPN (ESRK)<br>OLI<br>CPC | 7185111234<br>00<br>emergency | PAI (CBN obtained from MPC/GMLC) | <sip:+13125551234@carrier.example.net;user=phone> |
| NA | | Request URI | urn:service:sos |

### 9.4.5 CAMA MF WCM to SIP Header Mapping Example

Table 9-6 illustrates the mapping from CAMA MF signaling to SIP headers sent to the I-CSCF in the outgoing SIP INVITE message for Wireline Compatibility Mode wireless calls. The Called Party Number is mapped as shown in the table. The content of the MF Calling Number/ANI (i.e., the ESRK) is used to query the MPC/GMLC. The callback number received in the response from the MPC/GMLC is used to populate the From and PAI headers. The NPA is populated by the LNG based on the incoming trunk group.

**Table 9-6: CAMA MF WCM to SIP Header Mapping Example**

| CAMA Signaling | CAMA Example | SIP Header | SIP Example |
|---|---|---|---|
| Calling Number/ ANI (ESRK) | I+7digits<br>0+5111234 | From (CBN obtained from MPC/GMLC) | <sip:+13125551234@carrier.example.net;user=phone> |
| Called Number | 911 | To | sip:911@example.com |
| Calling Number/ ANI (ESRK) | I+7digits<br>0+5111234 | PAI (CBN obtained from MPC/GMLC) | <sip:+13125551234@carrier.example.net;user=phone> |
| NA | | Request URI | urn:service:sos |

### 9.4.6 FG D MF WCM to SIP Header Mapping Example

Table 9-7 illustrates the mapping from FG D MF signaling to SIP headers sent to the I-CSCF in the outgoing SIP INVITE message for Wireline Compatibility Mode wireless calls. The Called Party Number is mapped as shown in the table. The content of the MF Calling Number/ANI (i.e., the ESRK) is used to query the MPC/GMLC. The callback number received in the response from the MPC/GMLC is used to populate the From and PAI headers.

**Table 9-7: FG D MF WCM to SIP Header Mapping Example**

| FG D Signaling | FG-D Example | SIP Header | SIP Example |
|---|---|---|---|
| Calling Number/ ANI (ESRK) | II+10-digits<br>00+7185111234 | From (CBN obtained from MPC/GMLC) | <sip:+13125551234@carrier.example.net;user=phone> |
| Called Number | 911 | To | sip:911@example.com |

| FG D Signaling | FG-D Example | SIP Header | SIP Example |
|---|---|---|---|
| Calling Number/ ANI<br>(ESRK) | II+10-digits<br>00+7185111234 | PAI (CBN obtained from MPC/GMLC) | <sip:+13125551234@carrier.example.net;user=phone> |
| NA | | Request URI | urn:service:sos |

### 9.4.7 SS7 NCAS to SIP Header Mapping Example

Table 9-8 illustrates the mapping from SS7 parameters to SIP headers sent to the I-CSCF in the outgoing SIP INVITE message for NCAS wireless calls. The Called Party Number and Calling Party Number parameters are mapped as shown in the table.

**Table 9-8: SS7 NCAS to SIP Header Mapping Example**

| SS7 Parameter | SS7 Example | SIP Header | SIP Example |
|---|---|---|---|
| CPN<br>OLI<br>CPC | 3125554567<br>62<br>emergency | From | <sip:+13125554567@carrier.example.net;user=phone> |
| CdPN | 911 | To | sip:911@example.com |
| CPN<br>OLI<br>CPC | 3125554567<br>62<br>emergency | PAI | <sip:+13125554567@carrier.example.net;user=phone> |
| NA | | Request URI | urn:service:sos |

### 9.4.8 CAMA MF NCAS to SIP Header Mapping Example

Table 9-9 illustrates the mapping from CAMA MF NCAS signaling to SIP headers sent to the I-CSCF in the outgoing SIP INVITE message for NCAS wireless calls. The Called Number and Calling Number are mapped as shown in the table. The NPA is populated by the LNG based on the incoming trunk group.

**Table 9-9: CAMA MF NCAS to SIP Header Mapping Example**

| MF NCAS Signaling | MF NCAS Example | SIP Header | SIP Example |
|---|---|---|---|
| Calling Number/ANI | I + 7 Digits<br>0+5554567 | From | <sip:+13125554567@carrier.example.net;user=phone> |
| NA | | To | sip:911@carrier.example.com |
| Calling Number/ ANI | I + 7 Digits<br>0+5554567 | PAI | <sip:+13125554567@carrier.example.net;user=phone> |
| NA | | Request URI | urn:service:sos |

### 9.4.9 FG D MF NCAS to SIP Header Mapping Example

Table 9-10 illustrates the mapping from FG D MF NCAS signaling to SIP headers sent to the I-CSCF in the outgoing SIP INVITE message for NCAS wireless calls. The Called Number and Calling Number are mapped as shown in the table.

**Table 9-10: FG D MF NCAS to SIP Header Mapping Example**

| MF NCAS Signaling | MF NCAS Example | SIP Header | SIP Example |
|---|---|---|---|
| Calling Number/ANI | II + 10-digits<br>62+3125554567 | From | <sip:+13125554567@carrier.example.net;user=phone> |
| NA | | To | sip:911@carrier.example.com |
| Calling Number/ ANI | II + 10-digits<br>62+3125554567 | PAI | <sip:+13125554567@carrier.example.net;user=phone> |
| NA | | Request URI | urn:service:sos |

## *9.5 Procedures at the LPG*

To support emergency call delivery to legacy PSAPs, the LPG applies signaling and service-specific interworking functionality to emergency originations to allow the information provided in incoming SIP signaling to be delivered to the legacy PSAP in a form that it can process. Traditional MF and E-MF interfaces to legacy PSAPs assume that callback information signaled to a PSAP will be in the form of a 7/10-digit North American Numbering Plan (NANP) number. If the incoming SIP signaling contains callback information that is not in the form of (or easily converted to) a 10-digit NANP number, the LPG will perform a mapping from the non-NANP callback information to a locally-significant digit string (i.e., a pseudo Automatic Number Identification [pANI] of the form NPA/NPD-511-XXXX) that can be delivered to the legacy PSAP via traditional MF or E-MF signaling, with an appropriate NPA and II digits, or NPD.

Likewise, location information associated with an emergency call origination that is delivered to the LPG using SIP is expected to be in the form of a civic address or geodetic coordinates (if delivered “by-value”) or a reference URI (if delivered “by-reference”), rather than a NANP number. The LPG will therefore be expected to map this information to a location key (i.e., pANI) that is in the form of a NANP number (i.e., NPA/NPD-511-XXXX, with an appropriate NPA and II digits, or NPD) so that it can be delivered to legacy PSAPs that are interconnected to the LPG.

The LPG will also be capable of receiving and processing requests for initial and updated (caller) location, using existing NENA-defined ALI query protocols. If the location information received by the LPG in incoming SIP signaling is a LbyR, the LPG will have to send a dereference request to obtain the location information for the call before returning the location information in the appropriate format in the ALI response message.

There is additional information beyond just the callback number and location information that may be included in an ALI response. The LPG will use Additional Data structures to populate other fields in the ALI response. If Additional Data has been delivered to the LPG “by-reference,” the LPG will need to support the HTTP GET method described in IETF RFC 7230 [Ref 28] to obtain the Additional Data “by-value.” The LPG will use the information contained in the Call-Info header of the received INVITE to either identify the address of the target Additional Data Repository (ADR) to which the GET will be directed, or to identify the place in the message body where the Additional Data is provided “by-value”.

The LPG will interpret a switch-hook flash from a legacy PSAP as a request for emergency call transfer. The LPG will return a second dial tone to the legacy PSAP in response to the “flash” signal. The LPG will then be responsible for interpreting incoming DTMF signaling from the legacy PSAP to determine the transfer-to party for the call. Based on the information provided via DTMF, the LPG will identify the transfer-to party as follows:

- If the incoming DTMF signaling in the transfer request from the legacy PSAP consists of a 7/10 digit number, the LPG will use this information to identify the transfer-to party for the call.
- If the incoming DTMF signaling in the transfer request from the legacy PSAP consists of “# + 4 digits”, the LPG will add the appropriate NPA-NXX digits at the beginning of the 4-digit string, and use this information to identify the transfer-to party for the call.

- If the LPG receives a code of the form "*XX" in the DTMF signaling from the legacy PSAP, the LPG will do one of the following, based on trunk group provisioning:
  - The LPG will map the received *XX code to a static URI that is associated with the transfer-to party.
  - The LPG will map the received *XX code to a service URN, and query an ECRF using this service URN and the location information received with the call. The LPG will then use the URI returned in the response from the ECRF to identify the transfer-to party.

Having identified the transfer-to party, the LPG will follow the procedures specified in Clause 8.8 for transferring the emergency call.

The LPG will also be capable of processing transferred calls that are destined for legacy PSAPs that it serves. Incoming signaling associated with transferred calls from other PSAPs that are served by the same IMS-based NG9-1-1 Emergency Services Network will include a pointer/reference to an Emergency Incident Data Object (EIDO). The EIDO contains "Additional Data" that the primary PSAP has collected about the call, caller, and location, either based on incoming signaling or by direct interaction with the caller, and is expected to include callback information and location information. The LPG will send a dereference request to the primary i3 PSAP or serving LPG that generated the EIDO to obtain the data "by value". The LPG will use the same mechanisms defined for emergency originations to ensure that the callback and/or location information delivered to the legacy PSAP with the transferred call is in a format that the PSAP can process.

Also, the LPG will receive and must be able to process and respond to ALI requests from legacy PSAPs associated with emergency calls that have been transferred to them. The LPG will use the information provided in the EIDO to populate the ALI response. If the location information (or other information) in the EIDO is provided "by-reference", the LPG will have to first send a dereference request to obtain the information "by-value".

See Clause 6.2 of NENA-STA-010.3 [Ref 27] for further details related to LPG procedures and protocols.

## *9.6 Procedures at the IBCF*

The IBCF shall adhere to Clauses 4 and 5.10 in 3GPP TS 24.229 [Ref 2] with additions as noted below. In the IMS-based NG9-1-1 Service Architecture, the IBCF will be both the entry point to the network and the exit point from the network. The role performed by the IBCF (i.e., a proxy or B2BUA) will vary based on local policy. When acting as a B2BUA, the IBCF will follow the taxonomy of B2BUA roles described in RFC 7092 [Ref 33].

### 9.6.1 Entry Point IBCF

For emergency (9-1-1) originations, the entry point IBCF will perform normal border control functions. As described in Clause 5.10.10.2 of 3GPP TS 24.229 [Ref 2], when receiving an initial INVITE request containing one or more SIP Identity header fields, the IBCF shall determine the originating identity to be verified by decoding the Identity header field containing a SHAKEN PASSporT [Ref 48]. The IBCF shall also determine the RPH value to be verified by decoding the Identity header associated with the signed RPH. The IBCF will then build and send a verificationRequest to the STI-VS over the Ms reference point. The verificationRequest generated by the IBCF shall include an "identityHeader" parameter corresponding to the Identity header that contains the signed caller identity information in the SHAKEN PASSporT [Ref 48], an "identityHeaders" parameter corresponding to the Identity header that contains the signed RPH information, a "to" parameter that contains the destination identity from the To header, a "from" parameter containing the asserted identity from the From or P-Asserted-Identity, and a "time" parameter based on the Date header field in the incoming request. Upon receiving a verificationResponse with a "verstatValue" parameter reflecting the verification status of the Identity header associated with calling identity, the IBCF shall add a corresponding 'verstat' parameter to the verified identity in the SIP From header field or the SIP P-Asserted-Identity header field in the forwarded SIP request. If a verstat parameter is already present in the From or P-Asserted-Identity header of the received SIP INVITE, the entry IBCF must remove it. The entry IBCF shall also populate the verification results associated with the RPH in the Priority-Verstat header field of the outgoing SIP INVITE message, based on the associated verstatPriority parameter returned in the verificationResponse.

Once the IBCF validates the received SIP message and receives the results from the STI-VS it will forward the SIP INVITE to the I-CSCF. As the first active SIP element in an NG9-1-1 Emergency Services Network in the path of an emergency call, the IBCF must add the Call Identifier, Incident Tracking Identifier, and a Resource-Priority header set to “esnet.1” (if not already present) to the SIP INVITE message associated with the emergency call. The entry point IBCF will ensure that the Resource Priority Header is set to esnet.1 to indicate an emergency call. If an entry IBCF receives a SIP INVITE associated with a 9-1-1 call that contains a Resource-Priority header field set to a value other than “esnet.1”, the IBCF shall replace the invalid Resource-Priority header value with a value of “esnet.1”. If an Identity header associated with the invalid Resource-Priority header value is also present in the received INVITE, the IBCF shall delete the received Identity header. The IBCF should, based on local policy, interact with the STI-AS to have the updated Resource-Priority header value signed by sending a signingRequest to the STI-AS that contains an assertion value of “esnet.1”, along with the “orig”, “dest”, and “iat”. Note that the certificate used to sign the Resource-Priority header will be associated with the IMS-based Next Generation Emergency Services Network provider. Upon receiving 200 OK message from the STI-AS containing an identityHeader parameter associated with the signed Resource-Priority header, the IBCF shall populate the Identity header and the updated Resource-Priority header in the outgoing INVITE message associated with the emergency call.

If the entry IBCF receives an INVITE associated with a 9-1-1 call that does not contain an RPH, the IBCF shall add a Resource-Priority header set to “esnet.1” to the INVITE message. In this case, the IBCF need not sign the Resource-Priority header prior to passing the call to the I-CSCF.

In support of the transfer procedures described in Clause 8.8.1.1, the entry point IBCF will act as a signaling/media plane B2BUA that supports replacement of the Contact header and anchors media when the Supported header in the incoming INVITE message does not include the Replaces option tag.

For callback calls, the entry point IBCF will perform normal border control functions, and once the message is validated, it will forward the SIP INVITE to the Transit Function. If the SIP INVITE received by the entry point IBCF contains a verstat parameter in the From or P-Asserted-Identity header, the entry IBCF must remove it. As the first active SIP element in an NG9-1-1 Emergency Services Network in the path of a callback call, the IBCF must add a Resource-Priority header set to “esnet.0” (if not already present) to the SIP INVITE message associated with the callback call. Based on local policy, the entry point IBCF may also add an Origination-Id header to the SIP INVITE, indicating from where the request was received, as well as an Attestation-Info header.

For callback calls, the entry point IBCF in the interconnected network (i.e., the Service Provider network interconnected to the NG9-1-1 Emergency Services Network via the IP NNI) will perform normal border control functions, and once the message is validated, it will process the SIP INVITE as appropriate for that network.

The entry point IBCF shall not delete any P headers.

### 9.6.2 Exit Point IBCF

For an emergency (9-1-1) origination, the exit point IBCF shall use the Route header to determine the NENA i3 PSAP or the LPG. The IBCF shall pass all headers (including P headers) and message bodies unless passing of the parameters is prohibited with its role as a border gateway function. (See Clause 9.5 for further details related to the LPG.)

In support of the transfer procedures described in Clause 8.8.1.1, the exit point IBCF will act either as a proxy or as a B2BUA that does not modify the received To, From, or Contact header fields and does not terminate/anchor media (e.g., a Proxy-B2BUA).

In support of the transfer procedures described in Clause 8.8.1.2, the exit point IBCF will act as a signaling/media plane B2BUA that supports replacement of the Contact header and anchors media.

In support of callback calls, the exit point IBCF shall use the Route header to determine the well-known URI associated with the interconnected network. The IBCF shall pass all headers (including P headers) and message bodies unless passing of the parameters is prohibited with its role as a border gateway function. An exit point IBCF operating in an NG9-1-1 Emergency Services Network that supports caller identity authentication and RPH and SIP Priority header signing using the architecture described in Clause 7.3.2.2 will be responsible for interacting with an STI-AS to assert the telephone identity of the caller (i.e., the PSAP) and to request the signing of the RPH and SIP Priority header values prior to forwarding the callback request towards the succeeding network. An exit point IBCF that supports caller identity authentication and RPH/Priority header signing shall generate two signingRequest messages in an HTTP POST message. The signingRequest associated with the caller identity shall include an “attest” parameter and an “origid” parameter, populated according to local policy or based on information received by the IBCF in an Attestation-Info header and an Origination-Id header, respectively, within the SIP INVITE. The signingRequest associated with the caller identity shall also include "orig", "dest", and "iat" parameters. The signingRequest associated with the RPH and Priority header shall include an "rph" claim that contains an assertion value of "esnet.0", along with the "orig", "dest", and "iat", and an "sph" claim with a value of "psap-callback". The exit IBCF shall determine the assertion value for the "rph" and "sph" claims based on the RPH and Priority header received in the SIP INVITE message. The exit point IBCF shall use the "identityHeader" parameters associated with the caller identity and RPH/SIP Priority header returned in the signing responses within the HTTP 200 OK message from the STI-AS to populate Identity header fields in the outgoing SIP INVITE.

## *9.7 Procedures at the I-CSCF*

The I-CSCF shall adhere to Clauses 4 and 5.3 in 3GPP TS 24.229 [Ref 2] with additions and clarifications as noted in this Clause.

The I-CSCF receives emergency requests from the IBCF. The I-CSCF identifies that the incoming call is an emergency call if either of the following conditions is true.

- SIP INVITE contains a URI with "911" as the user part in the "To" header-field.
- SIP INVITE contains urn:service:sos in the Request URI.

Having identified the incoming call as an emergency call, the I-CSCF determines the address of the E-CSCF based on provisioned data.

The I-CSCF will route the emergency call to the E-CSCF based on the locally pre-configured E-CSCF address. The I-CSCF places the provisioned E-CSCF address in the Route header-field of the outgoing SIP INVITE.

## *9.8 Procedures at the Conferencing Application Server (AS)*

The conferencing Application Server (AS) shall adhere to Clause 5.2.3 in 3GPP TS 24.147 [Ref 11] with additions and clarifications as noted in this Clause.

When the transfer of an emergency call is initiated by a PSAP, the conferencing AS will receive a SIP INVITE message from an I-CSCF that contains a conference factory URI (that is known by/provisioned at the transfer-from PSAP or LPG) in the Request URI and To headers, and includes a Resource Priority Header set to "esnet.1" to indicate that the session request is associated with the transfer of an emergency call.

In response to the SIP INVITE message, the conferencing AS will interact with an MRFC and return a SIP 183 Session Progress message that includes a Contact header containing the conference URI for the conference that was allocated by the AS/MRFC, and the isfocus feature parameter. The conferencing AS will then return a SIP 200 OK message to establish the media session with the transfer-from PSAP.

If the conferencing AS subsequently receives a SIP SUBSCRIBE message from the transfer-from PSAP requesting a subscription to the conference associated with the URI obtained from the Contact header provided in the 180 SESSION PROGRESS message, the conferencing AS will return a SIP NOTIFY message providing subscription status information to the transfer-from PSAP.

In the context of emergency call transfer, the conferencing AS will receive REFER methods requesting that it invite other parties (e.g., the emergency caller, a transfer-to PSAP) to the conference. The REFER method will contain the Conf-ID and a Refer-To header. The Refer-To header may contain a URI with an escaped Replaces header field (e.g., if the REFER is associated with a request to invite an emergency caller to the conference), or the URI associated with the secondary transfer destination (e.g., transfer-to PSAP). If the REFER method is associated with a request to invite a transfer-to PSAP to the conference, it will also contain an escaped Call-Info header field containing a reference URI that points to the EIDO data structure and a purpose parameter of "eido".

The conferencing AS will return a 202 Accepted message in response to the REFER method, and will generate a SIP INVITE message toward the URI identified in the Refer-To header of the received REFER method to invite that party to the conference. If the conferencing AS does not have the capability to route the request toward the transfer-to PSAP, it will send the SIP INVITE to the Transit Function for routing. The SIP INVITE message will include the Conf-ID, and a Contact header that contains the conference URI and the isfocus feature parameter. If received in the associated REFER method, the SIP INVITE message generated by the conferencing AS will also contain the Replaces header or the Call-Info header field containing a reference URI that points to the EIDO data structure and a purpose parameter of "eido". The SIP INVITE message will include a Resource Priority Header set to "esnet.1" to indicate that the session request is associated with the transfer of an emergency call. The conferencing AS will also return a NOTIFY message to the transfer-from PSAP to update the status of the subscription associated with the REFER request.

If the conferencing AS receives a SIP SUBSCRIBE message from another entity that it has invited to the conference (e.g., a transfer-to PSAP), it will acknowledge the subscription request and respond with a SIP NOTIFY message containing subscription status information.

Upon receiving a SIP BYE message from any conference participant, the conferencing AS will terminate the connection to that party, and will provide updated status information to all subscribed participants.

## 9.9 Procedures at the Multimedia Resource Function Controller (MRFC)

In support of emergency call transfer in North America the MRFC shall support the procedures defined in Clause 5.2.2 of 3GPP TS 24.147 [Ref 11].

## 9.10 Procedures at the Multimedia Resource Function Processor (MRFP)

In support of emergency call transfer in North America, the MRFP shall provide the mixing of incoming media streams associated with multiple parties following the procedures specified in IETF RFC 4353 [Ref 13].

## 9.11 Procedures at the Transit Function

The Transit Function (TRF) shall adhere to the procedures described in Clause 5.19 of 3GPP TS 23.228 [Ref 19] with the clarifications as noted in this clause.

When a PSAP initiates the transfer of an emergency call toward a transfer-to PSAP, the conferencing AS may, as an operator option, communicate with a TRF to support routing of the session initiation request if the AS does not support the necessary routing capabilities. The TRF will be responsible for performing an analysis of the destination address, and determining where to route the session. The TRF is expected to route a session initiation request that is destined for a transfer-to PSAP via an IBCF.

When a PSAP initiates a callback call via an IMS-based NG9-1-1 Emergency Services Network, the TRF will be responsible for routing the callback call based on the destination address (i.e., the address associated with the emergency caller) received in incoming signaling. A Transit Function operating in an NG9-1-1 Emergency Services Network that supports caller identity authentication and RPH signing using the architecture described in Clause 7.3.2.1 shall be responsible for interacting with an STI-AS, by forwarding it the SIP INVITE, to assert the telephone identity of the caller (i.e., the PSAP) and to request the signing of the RPH and SIP Priority header values prior to forwarding the callback request towards the succeeding network via an exit point IBCF. The Transit Function shall pass the SIP INVITE received from the STI-AS to the exit point IBCF.

## 9.12 Procedures at the STI-AS

If the authentication architecture for callback calls described in Clause 7.3.2.1 is implemented, the STI-AS shall receive SIP INVITE messages associated with callback calls from a Transit Function and shall be responsible for determining, through service provider-specific means, the legitimacy of the telephone number identity and the RPH and SIP Priority header values being used in the INVITE. The STI-AS shall cryptographically sign the PASSporTs and add Identity header fields and signatures (corresponding the calling identity and RPH/SIP Priority header) to the SIP INVITE that it returns to the Transit Function.

If the authentication architecture for callback calls described in Clause 7.3.2.2 is implemented, the STI-AS shall receive signing requests in an HTTP POST message associated with callback calls from an exit point IBCF and shall be responsible for determining, through service provider-specific means, the legitimacy of the telephone number identity and the RPH and SIP Priority header values associated with the callback call. The STI-AS shall cryptographically sign the PASSporT and include identityHeader parameters and signatures (corresponding the calling identity and RPH/SIP Priority header) in the signing responses that it returns in an HTTP 200 OK message to the exit point IBCF.

If an entry IBCF in an IMS Next Generation Emergency Services Network replaces an invalid value in the Resource-Priority header field of an incoming INVITE message associated with a 9-1-1 call with the value “esnet.1” the STI-AS shall be capable of receiving and processing a signingRequest message from an entry IBCF that contains an assertion value of “esnet.1”, along with the “orig”, “dest”, and “iat”. As for the Resource-Priority header associated with a callback call, the STI-AS shall cryptographically sign the “rph” PASSporT and include an identityHeader parameter and signature corresponding to IMS-based Next Generation Emergency Services Network provider in the signingResponse that it returns in an HTTP 200 OK message to the entry point IBCF.

## 9.13 Procedures at the STI-VS

The STI-VS is an application server that performs the function of the verification service defined in RFC 8224 [Ref 36]. In the context of the IMS-based NG9-1-1 Service Architecture, the STI-VS provides verification services applicable to emergency calls destined for PSAPs that are served by an IMS-based NG9-1-1 Emergency Services Network. Upon receiving an HTTP POST containing a verificationRequest associated with an emergency (9-1-1) origination from an entry point IBCF in the IMS-based NG9-1-1 Emergency Services Network, the STI-VS shall retrieve the certificate referenced by the “x5u” field in the PASSporT protected header from the STI-CR. The STI-VS follows the basic certificate path processing as described in RFC 5280 [Ref 53], following the chain until the root is reached. The STI-VS ensures that the root certificate is on the list of trusted STI-CAs. The STI-VS validates the identityHeader parameter and identityHeaders parameter (if present) in the verificationRequest. In the context of emergency calling, the verificationRequest includes parameters associated with the SHAKEN claims and may also include an rph claim (if an associated Identity header is received). The verifier shall also follow the RFC 8224 [Ref 36] -defined verification procedures to check the corresponding date, originating identity and destination identities, with the restrictions specified in ATIS-1000074 [Ref 39] and the clarifications provided in Clause 7.3.1. If the calling telephone number identified in the P-Asserted-Identity or From header field is a non-dialable callback number formatted as described in Annex C of J-STD-036-C-2 [Ref 7], then the STI-VS shall canonicalize the calling telephone number to remove any leading ‘+’ sign or visual separators (i.e., “.”, “-“, “(“, and “)”), and use the resulting digit-string to check the "orig" claim. This special procedure shall be applied only if the non-dialable callback number is a digit-string of 10 digits with leading digits "911" or 11 digits with leading digits "1911". The STI-VS in the IMS-based NG9-1-1 Emergency Services Network shall return a “verstatValue” parameter and a “verstatPriority” parameter (if an “identityHeaders” parameter containing an “rph” claim is present in the verificationRequest) in the HTTP 200 OK message containing the verificationResponse to convey the results of the verification process. Depending on the results of the verification process, the “verstatValue” associated with the signed caller identity shall be set to “TN-Validation-Passed”, “TN-Validation-Failed”, or “No-TN-Validation”, and the “verstatPriority” associated with the signed RPH shall be set to “RPH-Validation-Passed”, “RPH-Validation-Failed”, or “No-RPH-Validation”. The STI-VS may include another appropriate indicator (not defined in this document) in the verificationResponse based on interactions with the CVT. The STI-VS must be invoked prior to terminating call processing associated with the emergency call.

# 10 Location Validation

Location validation is the validation of civic address-based location information against an authoritative GIS database containing only valid civic addresses obtained from 9-1-1 Authorities. “Validating” a location in NG9-1-1 means querying a Location Validation Function (LVF) to determine whether the location is suitable for use (specifically, if the location can be used to accurately route the call and dispatch responders). To be LVF ‘Valid’, a civic location must map to a location in the GIS database provisioned to the LVF such as a single address point, a single parcel / sub-parcel / building / floor / room polygon, or single point derived from an address-ranged road centerline layer (meaning the location is dispatchable). The civic address must be able to be mapped to a service area polygon of the type specified by the service URN in the validation request (meaning the location is routable). The LVF primarily returns a service mapping and lists of civic address elements that are considered valid, invalid, or were unchecked.

An underlying assumption of the NG9-1-1 Services Architecture is that 9-1-1 Authorities have transitioned from the tabular Master Street Address Guide (MSAG) and Emergency Service Numbers (ESNs) to a Geographic Information System (GIS)-based Location Validation Function (LVF) and RDF. Further, it is assumed that all civic locations will have been validated by the access network against the LVF prior to an emergency call being placed. In addition, it is expected that periodic revalidation of civic location against the LVF will be performed to assure that locations remain valid as changes in the GIS system that affect existing civic locations are made.

LVFs are queried using the LoST protocol. 9-1-1 Authorities provide authoritative LVFs both inside and outside of NG9-1-1 Emergency Services Networks. RFC 5222 [Ref 6], Clause 8.4.2, states that the inclusion of location validation is optional, and subject to local policy. All LoST server implementations deployed as an LVF must support the inclusion of location validation information in the “findServiceResponse” message. Local LVF policy is also responsible for determining which elements are given priority in determining which URI and which associated location data element tokens are deemed valid. To be “LVF-Valid”, a queried location using “urn:service:sos”, or “urn:emergency:service:sos”, or subservices of them must: 1) return a valid indication (i.e., no fields in the <invalid> list) from an LVF query with the location; and 2) must yield a single <mapping> element in the LoST response. In general, this means the fields supplied in the LoST query match exactly one location (one address point in the site/structure layer, or a valid house number in a road segment layer). An LVF must also support the validation of location around planned changes as defined by IETF draft-ietf-ecrit-lost-planned-changes [Ref 60].

The placement of LVF elements in an IP-enabled network varies with implementation. Since both end devices as well as LIS elements need to validate location, it is recommended that LVF elements are within the local domain or adjacent to it. Given that NG9-1-1 elements will also need to validate civic locations that either come with an emergency call, or are conveyed over the voice path, it is also a requirement that LVF elements be reachable from within any NG9-1-1 Emergency Services Network. LVF interaction at emergency call time may be performed by a PSAP to validate locations not received through incoming call signaling.

LVF elements are based on the LoST server architecture and as described above, use the LoST protocol (RFC 5222 [Ref 6]). The LVF is a logical function that may share the physical platform of an RDF; the LVF must share the same data for a given jurisdiction as the RDF. See Clause 9.3.1 for further discussion related to the provisioning of GIS data in RDFs and LVFs.

An LVF must be able to reach out to other LVFs in case of missing data, or in the case in which the requested location is outside its local jurisdiction, regardless of where it is deployed. If the LVF doesn’t know the answer, based on configuration, it will either refer a request for validation to one or more other LVFs, or it will iterate the request to some other LVF, providing the other LVF’s Uniform Resource Locator (URL) in the original LVF response. Redundant LVF elements are recommended in order to maintain a high level of availability and transaction performance.

See NENA-STA-010.3 [Ref 27] for further details related to the LVF.

# 11 Test Calls

The IMS-based NG9-1-1 Service Architecture should support the handling of 9-1-1 calls placed by a test-initiating device. The test mechanism should mimic the call path that would be used by an actual 9-1-1 call as closely as practical. An INVITE message with the Request-URI that contains a Service URN of “urn:service:test.sos” shall be interpreted by Functional Elements in an IMS-based NG9-1-1 Emergency Services Network as a request to initiate a test call. The PSAP will return a 200 OK response to indicate that it will complete the test function. See Clause 9 of NENA-STA-010.3 [Ref 27] for further information.

# 12 Logging

A logging function shall be used by all elements within the IMS-based NG9-1-1 Service Architecture to support the logging of all significant steps associated with the processing of an emergency call. This includes the logging of internal and external events, as well as media, and messages. All forms of media associated with emergency calls must be logged. Media recording should begin at the earliest point in the call path as possible. Recording may occur before the call has been answered if early media are available. It is desirable that recording of media associated with an emergency call occur both at or near the ingress to the IMS-based NG9-1-1 Emergency Services Network and within a PSAP.

The logging function incorporates a web service that supports logging and retrieving events. In addition to the web service interface, the logging function must implement the Session Recording Protocol interface, as defined in RFC 7866 [Ref 62] for recording media and, if provided, the associated metadata. The logging function must also provide a Real-time Streaming Protocol (RTSP) interface to play back the media. Clients to the logging function must support logging to at least two logging functions for redundancy purposes, with support for three (3) or more recommended.

Because events and media related to an Incident may be logged in several different logging functional elements during the life of the Incident, it may be necessary to query multiple logging functional elements to reconstruct what happened. The data stored in a logging functional element will contain raw statistical information that can be collated and compared with data from other systems to provide valuable insights into how the NG9-1-1 service is performing. Analysis of this data can guide resource allocation to support continual improvement of services. Policies and agreements will need to be established to facilitate appropriate sharing of these data.

See Clause 4.12 of NENA-STA-010.3 [Ref 27] for further details related to logging functionality.

# 13 Discrepancy Reporting

IMS-based NG9-1-1 Emergency Services Networks shall support a Discrepancy Report (DR) function to allow notifications to be exchanged between IMS elements and Public Safety entities to report data or configuration errors encountered during the processing of emergency calls. Consistent with NENA-STA-010.3 [Ref 27], the DR function is intended to be generated by any entity that is using data and detects a problem. In the context of IMS-based NG9-1-1 Emergency Services Networks, certain IMS elements shall support DR functionality to facilitate reporting under the following scenarios:

- An E-CSCF shall be capable of receiving and processing a DR from a PSAP if an emergency call is misrouted
- An LRF shall be capable of generating a DR to the owner of a routing policy (e.g., PSAP) that has a problem (e.g., formatting, syntax or other errors in the policy)
- An RDF shall be capable of generating a DR to a GIS entity due to an issue encountered with routing data populated in the RDF
- An E-CSCF or LRF shall be capable of filing a DR to the RDF due to an error encountered in the routing data provided for the emergency call
- A PSAP or LRF or LPG shall be capable of filing a DR to a Location Information Server (LIS) or Additional Data Repository (ADR) or originating network LRF if an error is detected in a response to a location or additional data dereference request
- An IBCF or E-CSCF or LRF shall be capable of sending a DR to an originating network if it receives signaling associated with an emergency call that is malformed
- IMS-based NG9-1-1 Emergency Services Network operators shall be capable of receiving DRs from any client related to general networking issues (e.g., high latency, packet loss, incorrect Domain Name System [DNS], or Dynamic Host Configuration Protocol [DHCP] behavior)
- Logging clients in IMS-based NG9-1-1 Emergency Services Networks shall be capable of filing a DR on the Logging Service
- Any entity might need to file a DR on another entity due to authentication issues (bad certificate, unknown entity, etc.)
- An E-CSCF or PSAP might need to file a DR on an IBCF.

When a discrepancy related to a network element (e.g., an E-CSCF) is reported, the DR is reported using a DR web service operated by the entity that operates that element, not necessarily by the element itself. Clause 3.7 of NENA-STA-010.3 [Ref 27] describes a standardized Discrepancy Reporting mechanism in the form of a web service. The OpenAPI description of this web service can be found in Appendix E.2.1 of NENA-STA-010.3 [Ref 27].

Discrepancy reporting is not intended to be an alarm function requiring immediate response. While an automated mechanism is specified to handle sending and receiving of DRs and the responses to those DRs, humans will usually be responsible for generating and acting on them.

All DRs must include the following data elements:

- Time Stamp of Discrepancy Submittal
- Discrepancy Report ID (a unique value generated by the reporting entity)

- Discrepancy reporting entity Fully Qualified Domain Name (FQDN)
- Discrepancy reporting agent user ID
- Discrepancy reporting contact info
- Service or Instance in which the discrepancy exists
- Discrepancy Report type (see Clause 3.7 of NENA-STA-010.3 [Ref 27])
- Additional notes/comments
- Reporting entity's assessment of severity
- DR-specific information as appropriate for the affected service or database

Details describing the service/database-specific content associated with discrepancy reports generated when specific errors/discrepancies are detected are described in Clauses 3.7.4 through 3.7.22 of NENA-STA-010.3 [Ref 27].

# 14 Security Considerations

IMS-based NG9-1-1 Emergency Services Networks are expected to be compliant with the security mechanisms described in NENA 75-001 [Ref 58], *Security for Next Generation 9-1-1 Standard (NG-SEC)* [Ref 58]. NENA 75-001 [Ref 58] emphasizes that network security is critical to the overall security posture of NG9-1-1. An improperly secured network opens NG9-1-1 entities up to intrusion by unauthorized machines or personnel, potentially leading to loss of service resulting in the inability to accept critical calls from the public. Improperly secured networks also provide a conduit for propagation of malicious or destructive code. Consistent with NENA 75-001 [Ref 58], firewalls must be established at all boundary points to control traffic in and out of an IMS-based NG9-1-1 Emergency Services network. Border gateways at the edge of an IMS-based NG9-1-1 Emergency Services Network will include firewall functionality to prevent unauthorized access to the network. Firewalls deployed in an NG9-1-1 Emergency Services Network shall provide application and network layer protection and scanning and Denial of Service (DoS) detection and protection (e.g., detection of unusual incoming IP packets that may then be blocked to protect the intended receiving user or network). To prevent Distributed Denial of Service (DDoS) attacks, the firewall should also support destination-specific monitoring, regardless of the source address.

IMS-based NG9-1-1 Emergency Services Networks are also expected to comply with the encryption and authentication mechanisms defined in NENA-STA-010 [Ref 27]. Based on NENA-STA-010 [Ref 27], each agency and each agent in an agency are issued credentials that allow them to be identified to all services in an ESInet. For PSAPs and 9-1-1 Authorities, the root Certificate Authority for agent and agency certificates is the PSAP Credentialing Agency (PCA). The certificate can be issued directly by the PCA, or the PCA can issue a certificate to an agency that, in turn, issues certificates to other agencies or agents. Consistent with NENA-STA-010 [Ref 27], all protocol exchanges across an IMS-based NG9-1-1 Emergency Services Network should be authenticated. Protocol operations are expected to use RSA-2048 encryption, with the credentials rooted in the PCA, typically over TLS. All elements in an NG9-1-1 Emergency Services Network must accept RSA-2048 with a certificate rooted in the PCA. Elements may accept alternate authentication cryptosystems as long as they are at least as strong as RSA-2048, but RSA-2048 must be supported by all implementations.

In addition, all protocol operations must be integrity-protected with TLS, using SHA-256 or stronger. All protocol operations must be privacy protected via TLS, preferably using Advanced Encryption Standard (AES) with a minimum key length of 256 bits (AES 256). Stored data which contains sensitive or confidential information must be stored encrypted, using AES 256 or an equivalently strong algorithm. (See Clause 5.8 of NENA-STA-010 [Ref 27] for further details.)

Cryptology choices must constantly be re-evaluated based on ongoing threat analysis, algorithm weakness research, and other factors. As new threats emerge, NG9-1-1 Emergency Services Networks may need to be upgraded to support enhanced algorithms that provide greater protection than the RSA- 2048, SHA-256, and AES 256 that is currently required.

Administrative access to IMS-based NG9-1-1 Emergency Services Networks must be controlled with appropriate identification, authentication and logging capabilities. Access control measures shall be utilized by all computer resources, systems, applications and networks to restrict access to sensitive information or system/network processors to authorized personnel only. Such measures could include the use of system configuration, file system permissions, system rights or access control software, etc.

Where possible access control shall be accomplished with “role-based” privileges that assign users to roles and grant access to members of a role rather than to individuals. Suspicious or unusual activity, which may indicate an attempt to breach the integrity of Public Safety networks and systems, shall be reported immediately to an established Security Point of Contact or equivalent. Any, and all, actual, attempted, and/or suspected misuse of Public Safety assets shall be reported immediately to the appropriate organizations.

See NENA 75-001 [Ref 58] and NENA-STA-010.3 [Ref 27] for further details regarding security considerations applicable to NG9-1-1 Emergency Services Networks.

# 15 Network Monitoring Thresholds

This clause describes default timeout thresholds for alerting and alarming for functional elements in an IMS-based NG9-1-1 Service Architecture. While the exact timeout thresholds used in a specific implementation of an IMS-based NG9-1-1 Service architecture will depend on physical infrastructure factors and practical experience, the values described in this clause may be viewed as recommended defaults. The thresholds are intended to provide guidance to assist those who will need to alert, alarm, or take some automated action when a transaction timeout occurs. Typically, the initiator of a transaction or a monitoring application will raise an alert or alarm if the responding entity takes too long to respond. The metrics described in this clause are based on the information provided in NENA-INF-040.2, *NENA Managing & Monitoring NG9-1-1 Information Document* [Ref 59]. Only the metrics specific to an IMS-based NG9-1-1 Emergency Services Network, as illustrated in Figure 7-2, are described here. For metrics relevant to a Legacy Network Gateway (LNG), see Clause 2.2.6.1 of NENA-INF-040.2 [Ref 59]. For metrics relevant to a Legacy PSAP Gateway (LPG), see Clause 2.2.6.5 of NENA-INF-040.2 [Ref 59].

NENA-INF-040.2 [Ref 59] describes the thresholds associated with various transactions relevant to the processing of a 9-1-1 call in terms of: the normal upper boundary measurement of time elapsed between the point at which the transaction is initiated and a response is received (i.e., a Monitor Event); the recommended time when a notification-worthy error event is deemed to have occurred due to a value greater than the normal expected transaction time (i.e., an Error Event); and if a Monitor Event must occur more than once to trigger an Error Event, the number of occurrences required before a notification should be sent to the appropriate parties to ensure the timely initiation of any corrective actions for the Error Event.

When a 9-1-1 call is received by an entry IBCF in an IMS-based NG9-1-1 Emergency Services Network, the IBCF will determine whether the associated INVITE message contains one or more Identity headers. If an Identity header is present in the received INVITE, the IBCF shall initiate an interaction with an STI-VS to verify the information in the Identity header(s). The time between an IBCF sending a verification request to an STI-VS, and it receiving a response from the STI-VS should be a maximum of 1000 ms. If, after 1000 ms, the IBCF has not received a response from the STI-VS, an Error Event (i.e., an event that is considered a serious or fatal error requiring prompt action) should be detected by the IBCF, and a notification (i.e., an alert) should be generated. According to NENA-INF-040.2 [Ref 59], no retries should be attempted.

If an entry IBCF in an IMS-based NG9-1-1 Emergency Services Network receives an INVITE message that contains an Identity header associated with a signed Resource-Priority Header (RPH) and the RPH contains a value other than “esnet.1”, the IBCF will delete the Identity header and replace the contents of the RPH with the value “esnet.1”, as described in Clause 9.6.1. Based on local policy, the IBCF may send a signing request to the STI-AS with the new RPH value. The time between the IBCF sending the signing request and the IBCF receiving a response from the STI-AS should be a maximum of 500 ms. If, after 500 ms, the IBCF has not received a response from the STI-AS, an Error Event should be detected by the IBCF, and a notification should be generated. According to NENA-INF-040.2 [Ref 59], no retries should be attempted. If the IBCF interacts with the STI-AS, it will use the response from the STI-AS to create an Identity header associated with the RPH.

NENA-INF-040.2 [Ref 59] also describes timers associated with call setup (i.e., the time between a SIP INVITE being sent and the first response being received). From the perspective of an IBCF in an IMS-based NG9-1-1 Emergency Services Network, the time between an INVITE associated with a 9-1-1 call being sent by an entry IBCF to an I-CSCF and the first response being returned by the I-CSCF (e.g., 100 Trying or other response) should have maximum time of 100 ms, as specified in NENA-INF-040.2 [Ref 59]. An INVITE may be retransmitted up to 5 additional times (for a total of 6 instances). As described in RFC 3261 [Ref 18], the time between retries will double with each successive retry. An Error Event should be detected by the IBCF if the transaction timer reaches 6300 ms. At that point a notification should be triggered (i.e., an alert should be sent). The same thresholds apply for INVITE messages sent by an I-CSCF to an E-CSCF, from an E-CSCF to an exit IBCF, and from an exit IBCF to an i3 PSAP Call Handling Function or LPG.

In the context of an IMS-based NG9-1-1 Emergency Services Network architecture, an LRF will act as a redirecting server for an E-CSCF. Consistent with the call setup times described above, it is expected that the E-CSCF will send an INVITE to the LRF and will received a 100 Trying response within a maximum time of 100 ms, as specified in NENA-INF-040.2 [Ref 59]. The INVITE may be retransmitted up to 5 additional times (for a total of 6 instances), with an alert notification triggered if the transaction timer reaches 6300 ms. An additional metric associated with interactions between an E-CSCF and an LRF must consider all of the interactions that an LRF may have with other functional elements when processing an emergency call. Upon receiving the INVITE from the E-CSCF, the LRF may need to initiate a dereference request if the location information in the INVITE is a location-by-reference. The LRF will then need to interact with the RDF to determine the location-based routing for the call, and may also consult Policy Routing Rules before determining the routing information that will be returned to the E-CSCF. If the Policy Routing Rules are dependent on Additional Data and the Additional Data in the INVITE from the E-CSCF was sent “by reference”, the LRF will need to send a dereference request to the appropriate Additional Data Repository (ADR). Thus, the threshold defined for an E-CSCF to receive a 300 Multiple Choices message from the LRF in response to the INVITE that it forwards to an LRF must take into account all of the thresholds associated with the interactions that an LRF may have with an LRF/Location Information Server (LIS) in an originating IP network (or an LNG if the originating network is a legacy network) to support location dereference transactions, interactions with ADRs to support Additional Data dereference transactions, interactions between the LRF and the RDF to support routing determination transactions, as well as any Policy Routing it may perform. (See Annex C for an analysis of how the thresholds described below were calculated.)

If the location information received by the LRF in an INVITE from an E-CSCF is a location-by-reference, the LRF will initiate a HELD dereference request to the target identified by the location URI conveyed in the Geolocation header field of the INVITE. The time between an LRF in an IMS-based NG9-1-1 Emergency Services Network initiating a location dereference request to an LRF or LIS in an IP originating network (or an LNG in the case of a legacy originating network), and the LRF (in the IMS-based NG9-1-1 Emergency Services Network) receiving the location data or an error response is expected to have a maximum time of 1 sec, as specified in NENA-INF-040.2 [Ref 59]. If no response is received after 1 second, a second location dereference request should be initiated. An Error Event should be detected by the LRF if the location dereference transaction timer reaches 2 sec. At that point, a notification should be triggered (i.e., an alert should be sent).

Based on NENA-INF-040.2 [Ref 59], the time between the LRF issuing the LoST query to the RDF and the response being received from the RDF should have a default value of 300 ms. If no response is received after 300 ms, a single retry should be attempted. If, after a total of 600 ms, the LRF has not received a response from the RDF, a notification should be triggered.

If the LRF issues an Additional Data dereference request, the default value for the time between the LRF issuing the Additional Data dereference request and the ADR returning the data or error response is 1 second. If a response is not received within this timeframe, a single retry should be attempted. If, after 2 seconds, a response has not been received, an Error Event should be detected, and an alert should be sent.

Taking into account the various activities that may be performed by the LRF before it returns a 300 Multiple Choices response to the E-CSCF, the transaction timer set by the E-CSCF associated with receipt of a 300 Multiple Choices message from an LRF should have a default maximum value of 3000 ms. An INVITE may be retransmitted up to 1 additional time (for a total of 2 instances). An Error Event should be detected by the E-CSCF if the transaction timer reaches 5200 ms. At that point a notification should be triggered.

**Annex A**
(normative)

# A SIP INVITE Profile for Emergency Calls

This normative annex provides the SIP INVITE profile for emergency calls received at the IBCF in the ingress side of the IMS-based NG9-1-1 Emergency Services Network and sent to a NENA i3 PSAP. Headers not included in this table are not pertinent to emergency calls and may be ignored.

**Table A-1: SIP INVITE Header Profile Legend**

| Code | Code Name | Sending Side | Receiving Side |
|---|---|---|---|
| M | Mandatory | The capability shall be supported.<br>It is a static view of the fact that the conformance requirements related to the capability in the reference specification are mandatory requirements. This does not mean that a given behavior shall always be observed, but that it shall be observed when the implementation is placed in conditions where the conformance requirements from this document compel it to do so. For instance, if the support for a header in a sent request or response is mandatory, it does not mean that it shall always be present, but that it shall be present according to the description of the behavior in this document. | Same as in the sending side with the following additions:<br>Processing should not continue if required information is unavailable. (Suitable disconnection/release processing should be performed.)<br>However, when a default value has been decided upon, processing is performed using the default value. |
| O | Optional | The capability may or may not be supported. It is an implementation choice. | Same as in the sending side with the following additions:<br>If possible, perform the processing expected by the sending side.<br>When the processing expected by the sending side cannot be performed, the received content should be ignored and processing should continue. |
| - | Not Supported | The capability is not supported or beyond the scope of this standard. | The capability is not supported or beyond the scope of this standard. |
| S | Recommended | The capability should be supported.  It is an implementation choice. | Same as in the sending side with the following additions:<br>If possible, perform the processing expected by the sending side.<br>When the processing expected by the sending side cannot be performed, the received content should be ignored and processing should continue. |

The following identifies the use of the columns:

- **Header** – Header name.
- **Send PSAP** – Headers sent to NENA i3 PSAP via the egress IBCF.
- **Recv IBCF** – Headers Received at the ingress IBCF.

- **Reference and Notes** – Reference RFCs and clarifying notes.

**Table A-2: SIP INVITE Header Profile**

| Header | Send PSAP | Recv IBCF | Reference and Notes |
|---|---|---|---|
| Accept | O | O | RFC 3261 [Ref 18] Clause 20.1. |
| Accept-Encoding | O | O | RFC 3261 [Ref 18] Clause 20. 2. |
| Accept-Language | O | O | RFC 3261 [Ref 18] Clause 20.3.<br>The "Accept-Language" header MAY be present in requests with a value of "en" for English, which should be supported. Other values MAY be supported. |
| Allow | S | S | RFC 3261 [Ref 18] Clause 20.5.<br>The header value should list all supported methods, i.e., at a minimum, "INVITE", "ACK", "CANCEL", "BYE", "OPTIONS", and "PRACK". |
| Attestation-Info | O | O | 3GPP TS 24.229 Clause 7.2.18 |
| Call-ID | M | M | RFC 3261 [Ref 18] Clause 20.8. |
| Call-Info | O | O | RFC 3261 [Ref 18] Clause 20.9 and Clause 9.1.1 of this standard.<br>If a Call-Info header is received at the ingress IBCF or created by the LNG, it will be passed unaltered through the egress IBCF toward the PSAP. |
| Contact | M | M | RFC 3261 [Ref 18] Clause 20.9. |
| Content-Language | O | O | RFC 3261 [Ref 18] Clause 20.13. |
| Content-Length | M | M | RFC 3261 [Ref 18] Clause 20.14. |
| Content-Type | M | M | RFC 3261 [Ref 18] Clause 20.15, RFC 6442 [Ref 15] Clause 5.1.<br>The value of "multipart/mixed" MUST be supported.  The value of "application/sdp" MUST be supported. The value of "application/pidf+xml" MAY be supported and MUST be supported if LbyV is included in the body of the SIP INVITE message. |
| Cseq | M | M | RFC 3261 [Ref 18] Clause 20.16. |
| From | M | M | RFC 3261 [Ref 18] Clause 20.20. |
| Geolocation | M | M | RFC 6442 [Ref 15] Clause 4.1 and Clause 9.1.1 of this standard. |
| Geolocation-Routing | M | M | RFC 6442 [Ref 15] Clause 4.2 and Clause 9.1.1 of this standard. |
| History-Info | O | O | RFC 7044 [Ref 23]. |
| Identity | M | O | RFC 8224 [Ref 36]<br>The Identity header may be received by the IBCF on the ingress side of the NG9-1-1 Emergency Services Network, and if received, must be signaled to the NENA i3 PSAP via the egress IBCF. |
| Max-Forwards | M | M | RFC 3261 [Ref 18]Clause 20.22.<br>When the IBCF implementation of a back-to-back User Agent (B2BUA) forwards a request, it MUST use a Max-Forwards value equal to the incoming Max-Forwards value minus one. |
| MIME-Version | O | O | RFC 3261 [Ref 18] Clause 20.24.<br>The version "1.0" value is the default; other values MAY be supported. |
| Origination-Id | O | O | 3GPP TS 24.229 [Ref 2] Clause 7.2.19 |

| Header | Send PSAP | Recv IBCF | Reference and Notes |
|---|---|---|---|
| P-Access-Network-Info Header | O | O | RFC 3455 [Ref 24] Clause 4.4.1. |
| P-Asserted-Identity | O | O | RFC 3325 [Ref 25] Clause 4 and Clause 9.1.1 of this standard. |
| P-Charging-Vector Header | O | O | RFC 3325 [Ref 25] Clause 4.6.<br>If the P-Charging-Vector header is included in the incoming SIP INVITE it is expected that it identifies the originating carrier. |
| Record-Route | M | O | RFC 3261 [Ref 18] Clause 20.30. |
| Reply-To | - | - | RFC 3261 [Ref 18] Clause 20.31. |
| Require | O | O | RFC 3261 [Ref 18] Clause 20.32.<br>The option tags “precondition”, “replaces”, and “100rel” MUST be supported. |
| Resource-Priority | M | O | RFC 4412 [Ref 20], updated by RFC 7134 [Ref 21]. |
| Route | M | O | RFC 3261 [Ref 18] Clause 20.34 and Clause 9.1.1 of this standard. |
| Supported | M | M | RFC 3261 [Ref 18] Clause 20.37.<br>The values “precondition”, “replaces” and “100rel” may be supported. However, a value present in the "Require" header SHOULD NOT also be present in the Supported header. |
| To | M | M | RFC 3261 [Ref 18] Clause 20.39. |
| Unsupported | O | O | RFC 3261 [Ref 18] Clause 20.40. |
| Visa | M | M | RFC 3261 [Ref 18] Clause 20.42. |

**Annex B**
(informative)

# B Message Examples

This informative Annex provides message examples for various use cases.

## *B.1 Legacy Fixed Line UE to Traditional Legacy PSAP (Wireline) Example*

The following represents an example of a SIP INVITE sent from the LNG to the BCF of the emergency services network for an emergency call originating from a fixed-line UE.

NOTES:

1. INVITE messages between the BCF and I-CSCF, between the I-CSCF and the E-CSCF, and between the E-CSCF and the LRF are the same except for providing the Via headers and the value of the Route header.
2. The INVITE message between the E-CSCF and the LPG (ignoring the BCF) are the same except for providing the Via headers and a Route URI obtained from the Contact header of the 300 Multiple Choices from the LRF.

```
INVITE urn:service:sos SIP/2.0
Via: SIP/2.0/UDP lng.provider.example.net;branch=z9hG4bK77993dd
Route: sip:i-cscf.es-provider.example.net;lr
From: <sip:+13125551234@lng.provider.example.net;user=phone>;tag=23ac
To: sip:911@esnet.example.net
Contact: sip:+13125551234@lng.provider.example.net;user=phone
P-Asserted-Identity: sip:+13125551234@lng.provider.example.net;user=phone
Geolocation: <cid:target-loc@lng.provider.example>
Geolocation-Routing:yes
Call-Info: “urn:nena:uid:callid:a56e556d871:lng.lng-provider”;purpose= nena-
CallId
Call-Info: “urn:nena:uid:incidentid:b34e556d225:lng.lng-provider”;purpose=
nena-IncidentId
Call-Info: <cid:ProviderInfo@lng.provider.example>;
purpose=EmergencyCallData.ProviderInfo
Call-Info: <cid:ServiceInfo@lng.provider.example>;
purpose=EmergencyCallData.ServiceInfo
Max-Forwards: 68
Call-ID: 19dn30
CSeq: 1 INVITE
Supported: 100rel, geolocation
Accept: application/sdp, application/pidf+xml, application/xml
Content-Type: multipart/mixed;boundary=boundary1
Content-Length: nn
--boundary1
Content-Type:application/sdp
[SDP here]
--boundary1
Content-Type: application/pidf/xml
Content-ID: target-loc@lng.provider.example
[PIDF-LO here]
--boundary1
Content-Type: application/xml
Content-ID: ProviderInfo@lng.provider.example
[Provider Information here]
--boundary1
Content-Type: application/xml
Content-ID: ServiceInfo@lng.provider.example
```

```
[Service Information here]
--boundary1--
```

The following represents an example of a 300 Multiple Choices sent from LRF to E-CSCF for an emergency call originated from a fixed-line UE and destined to a legacy PSAP via a LPG.

NOTE:

1. If the emergency request were destined to a NENA i3 PSAP the only change would be the IP address of the NENA i3 PSAP in the Contact header.

```
SIP/2.0 300 Multiple Choices
Via: SIP/2.0/UDP e-cscf.es-provider.example.net;branch=z9hG4bKk9eb5810k
Via: SIP/2.0/UDP i-cscf.es-provider.example.net;branch=z9hG4bK776asdhds
Via: SIP/2.0/UDP bcf.es-provider.example.net; branch=z9hG4bKdko11i5i71 Via:
SIP/2.0/UDP lng.provider.example.net; branch=z9hG4bK77993dd
From: <sip:+13125551234@lng-provider.example.net;user=phone>;tag=23ac>
To: urn:service:sos
Call-ID: 19dn30
CSeq: 1 INVITE
Contact:<sip:psap.st.county.lpg@provider.example.net>
Content-Length: 0
```

## *B.2 Legacy Mobile UE to Traditional Legacy PSAP (Wireless) Example*

Emergency call requests from a legacy mobile UE will enter the emergency services network providing a location reference for the LbyR scenario. The SIP will appear as in the B1 example with a different Geolocation header format as shown below. Otherwise the format is the same as shown in the B1 example.

```
Geolocation: <https:lng.provider.example/ajm4392>
Geolocation-Routing:yes
```

The 300 Multiple Choices response is the same as shown in the B1 example.

## *B.3 Fixed Line IP OSP UE to Traditional Legacy PSAP Example*

In this example the UE resides within an IP OSP network capable of providing the LbyV in the call request. The B1 example applies with the exceptions noted below.

1. The nena-CallId and nena-IncidentId are not provided by the OSP network.
2. The Via, Geolocation and other header examples represent the OSP network rather than the LNG.

Via example:

```
Via: SIP/2.0/UDP bcf.osp.provider.example.net; branch=z9hG4bK77993dd
```

Geolocation example:

```
Geolocation: <cid:target-loc@osp.provider.example>
```

The 300 Multiple Choices response is the same as shown in the B1 example.

## B.4 Mobile IP OSP UE to Traditional Legacy PSAP Example

In this example the UE resides within an IP OSP network capable of providing the LbyR in the call request. The B2 example applies with the exceptions noted below.

1. The nena-CallId and nena-IncidentId are not provided by the OSP network.
2. The Via, Geolocation and other header examples represent the OSP network rather than the LNG.

Via example:

```
Via: SIP/2.0/UDP bcf.osp.provider.example.net; branch=z9hG4bK77993dd
```

Geolocation example:

```
Geolocation: <https:osp.provider.example/ajm4392>
```

The 300 Multiple Choices response is the same as shown in the B1 example.

**Annex C**
(normative)

# C Analysis of Network Monitoring Thresholds in IMS-based NG9-1-1 Emergency Services Network

The E-CSCF to LRF reference point (Ml) equivalent within the NENA i3 architecture is an internal function to the ESRP; therefore, a recommended monitoring threshold is not available that can be mapped from NENA-INF-040.2 [Ref 59] to this standard. This analysis provides a recommendation for the default E-CSCF to LRF monitoring threshold of 3000ms for the transaction in which the E-CSCF sends an INVITE to the LRF and the LRF returns a 300 Multiple Choices response, taking into consideration lower-level LRF procedures with their own monitoring thresholds that must execute sequentially and in parallel within each E-CSCF to LRF SIP Redirect including retransmissions.

The lower-level procedures within the E-CSCF to LRF SIP Redirect to budget time for are:

1. LRF to LIS HELD Routing Location Dereference Request
2. LRF to RDF LoST Request (Sequential to Procedure 1)
3. LRF to ADR Additional Data Dereference Requests (Can occur in parallel to procedures 1 and 2)
4. LRF to PRF for determining final next hop URI (Sequential to Procedure 1, 2, and 3)

One-time retransmission is recommended when the first transaction times out; however, the maximum threshold is recommended to be 5200ms at which point a notification is triggered.

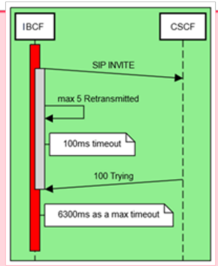
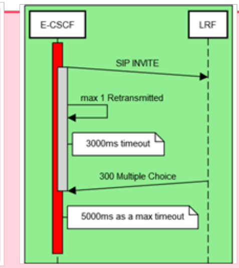
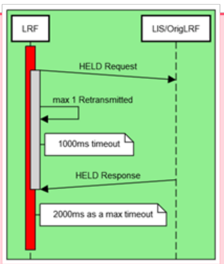
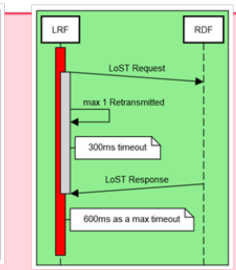
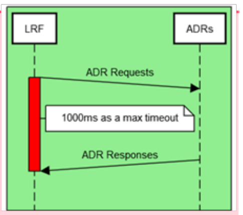
| Network Element | IBCF to I-CSCF,I-CSCF to E-CSCF, E-CSCF to LRF ,E-CSCF to IBCF,IBCF to IBCF,IBCF to LPG | E-CSCF to LRF | LRF to LIS/OrigLRF | LRF to RDF | LRF to ADRs |
|---|---|---|---|---|---|
| Signal Flow |  IBCF<br>CSCF<br>SIP INVITE<br>max 5 Retransmitted<br>100ms timeout<br>100 Trying<br>6300ms as a max timeout |  E-CSCF<br>LRF<br>SIP INVITE<br>max 1 Retransmitted<br>3000ms timeout<br>300 Multiple Choice<br>5000ms as a max timeout |  LRF<br>LIS/OrigLRF<br>HELD Request<br>max 1 Retransmitted<br>1000ms timeout<br>HELD Response<br>2000ms as a max timeout |  LRF<br>RDF<br>LoST Request<br>max 1 Retransmitted<br>300ms timeout<br>LoST Response<br>600ms as a max timeout |  LRF<br>ADRs<br>ADR Requests<br>1000ms as a max timeout<br>ADR Responses |
| Timeout | 100ms | X ms configurable (3000ms) | 1000ms | 300ms | 1000ms |
| Retransmission | 5 x retransmitted | 1 x retransmitted | 1 x retransmitted | 1 x retransmitted | 1 x retransmitted |
| Notification triggered | Max 6300ms | Z ms configurable (5200ms) | Max 2000 ms | Max 600ms | Max 2000ms |
| Notes | Retransmitted at 0.1s, 0.3s, 0.7s, 1.5s, 3.1s | IMS-Based(E-CSCF & LRF) equivalent to NENAi3 ESRP | | Including ECRF inquiry with Forest Guide | *All ADR dereferences shall be completed in this timer |

**Figure C.1: Call Setup, Call Routing and Dereferencing Transactions**

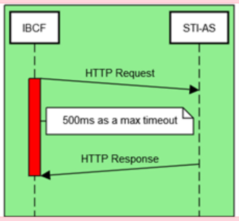
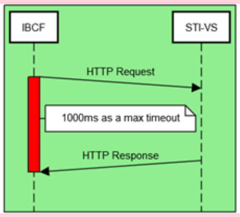
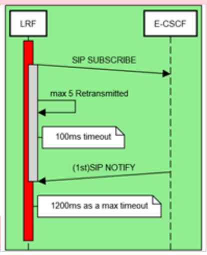
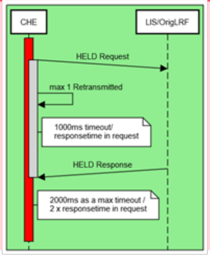
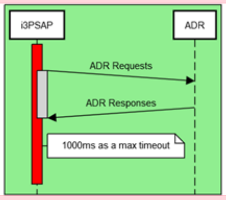
| Network Element | IBCF to STI-AS | IBCF to STI-VS | LRF to E-CSCF | CHE to LIS/Orig LRF (out of scope) | CHE to ADR (out of scope) |
|---|---|---|---|---|---|
| Signals |  IBCF<br>STI-AS<br>HTTP Request<br>500ms as a max timeout<br>HTTP Response |  IBCF<br>STI-VS<br>HTTP Request<br>1000ms as a max timeout<br>HTTP Response |  LRF<br>E-CSCF<br>SIP SUBSCRIBE<br>max 5 Retransmitted<br>100ms timeout<br>(1st)SIP NOTIFY<br>1200ms as a max timeout |  CHE<br>LIS/OrigLRF<br>HELD Request<br>max 1 Retransmitted<br>1000ms timeout/ responsetime in request<br>HELD Response<br>2000ms as a max timeout / 2 x responsetime in request |  i3PSAP<br>ADR<br>ADR Requests<br>ADR Responses<br>1000ms as a max timeout |
| Timeout | 500ms | 1000ms | 100ms | 1000m/responsetime in request | 1000ms |
| Retransmission | N/A | N/A | 5 x retransmitted | 1 x retransmitted | 1 x retransmitted |
| Notification triggered | 500ms | 1000ms | Max 6300ms | 2000m/ 2xresponsetime | Max 2000ms |
| Notes |  | Consider STI-VS has to retrieve key if P-key is not cached and process time with CVT |  |  |  |

**Figure C.2: Other Transactions**