
**ATIS-0500046**

# Analysis of Non-IP Call Authentication Mechanisms in Support of Emergency Services

**TECHNICAL REPORT**

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the All-IP transition, 5G, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.




ATIS-0500046, *Analysis of Non-IP Call Authentication Mechanisms in Support of Emergency Services*

*Published by*

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

**ATIS-0500046**

ATIS Technical Report on

# Analysis of Non-IP Call Authentication Mechanisms in Support of Emergency Services

**Alliance for Telecommunications Industry Solutions**

Approved March 28, 2022

**Abstract**

This Technical Report analyzes non-Internet Protocol (IP) call authentication mechanisms to determine their applicability to the handling of 9-1-1 calls in the context of Enhanced 9-1-1 (E9-1-1) and transitional Next Generation 9-1-1 (NG9-1-1) architectures.

## Foreword

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global information and communications technology (ICT) companies to advance the industry's most-pressing business priorities. ATIS serves the public through improved understanding between carriers, customers, and manufacturers.

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.

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

At the time of initiation or issuance of the letter ballot for this document, the committees responsible for its development had the following leadership:

D. Morkunas, ESIF 1st Vice Chair (Intrado)

J. Torres, ESIF 1st Vice Chair (Verizon Wireless)

B. Abley, ESIF 2nd Vice Chair (NENA)

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

E. Amoah, ESIF NGES Co-Chair (Verizon Wireless)

The **NGES** Subcommittee was responsible for the development of this document.

**Table of Contents**



**Table of Figures**

ATIS Standard on –

# Analysis of Non-IP Call Authentication Mechanisms in Support of Emergency Services

## 1 Scope, Purpose, & Application

### *1.1 Scope*

Regulators and industry stakeholders initially focused on supporting caller identity authentication and verification for calls carried over Internet Protocol (IP) networks using the Session Initiation Protocol (SIP) to address concerns related to robocalling and illegitimate caller identity spoofing. Caller authentication techniques, such as those described in ATIS standards related to Signature-based Handling of Asserted Information Using toKENs (SHAKEN) and IETF RFCs related to Secure Telephone Identity Revisited (STIR), have been developed to allow calls traveling through interconnected IP-based carrier networks to have the legitimacy of the caller's identity evaluated by the originating carrier and validated by the terminating carrier, facilitating the delivery of an indication of the legitimacy of the caller identity information to the called party. The ATIS Non-IP Call Authentication Task Force has defined call authentication mechanisms that will operate in the non-IP portions of voice service provider networks that may be useful in supporting the Second Report and Order [Ref 1] adopted and released by the Federal Communications Commission (FCC) on October 1, 2020.

This Technical Report discusses call authentication in the context of emergency services offered using legacy Enhanced 9-1-1 (E9-1-1) and transitional Next Generation 9-1-1 (NG9-1-1) architectures. It considers non-IP call authentication mechanisms that are being defined in a non-emergency context by the industry and discusses the impacts of call authentication on the processing of 9-1-1 calls.

### *1.2 Purpose*

This Technical Report provides an analysis of the applicability of non-IP call authentication mechanisms being considered by the industry to legacy E9-1-1 and transitional NG9-1-1 architectures.

### *1.3 Application*

This Technical Report applies to emergency (9-1-1) calls that originate in legacy networks and are routed via legacy Selective Routers (SRs) to legacy Public Safety Answering Points (PSAPs), as well as emergency (9-1-1) calls that originate in legacy networks and are routed via NG9-1-1 Emergency Services Networks to legacy or NG PSAPs. In addition, this Technical Report applies to emergency (9-1-1) calls that originate in IP Multimedia Subsystem (IMS) networks in North America and are routed via legacy SRs to legacy PSAPs, and emergency (9-1-1) calls that originate in IMS networks and are routed via NG9-1-1 networks to legacy PSAPs.

## 2 References

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

[Ref 1] Federal Communications Commission. *Second Report and Order In the Matter of Call Authentication Trust Anchor* (WC Docket 17-97). FCC 20-136.[1]

[Ref 2] ATIS-1000096, *Signature-Based Handling of Asserted Information Using Tokens (SHAKEN): Out-of-Band PASSporT Transmission Involving TDM Networks.*[2]

[Ref 3] draft-ietf-stir-servprovider-oob-01, *Out-of-Band STIR for Service Providers*.[3]

[Ref 4] ATIS-1000095, *Extending STIR/SHAKEN over TDM.*[2]

[Ref 5] ATIS-1000679, *Interworking Between Session Initiation Protocol (SIP) and ISDN User Part.*[2]

[1] This document is available from the Federal Communications Commission (FCC) at: < http://www.fcc.gov/ >.

[2] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS) at: < https://www.atis.org/ >.

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

[Ref 6] ATIS-0700015, *ATIS Standard for Implementation of 3GPP Common IMS Emergency Procedures for IMS Origination and ESInet/Legacy Selective Router Termination*. [2]
[Ref 7] ATIS-1000628, *Emergency Calling Service*. [2]
[Ref 8] NENA-STA-015.10-2018, *NENA Standard Data Formats for E9-1-1 Data Exchange & GIS Mapping*.[4]
[Ref 9] ATIS-1000074, *Signature-based handling of Asserted information using toKENs (SHAKEN)*. [2]
[Ref 10] 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*.[5]
[Ref 11] ITU-T Recommendation Q.763 (12/1999), *Signalling System No. 7 – ISDN user part formats and codes*.[6]
[Ref 12] ATIS-1000113, *Signaling System No. 7 (SS7) – Integrated Services Digital Network (ISDN) User Part*. [2]
[Ref 13] ATIS/TIA J-STD-036-C-2, *Enhanced Wireless 9-1-1 Phase II*. [2]
[Ref 14] NENA-STA-010.3-2021, *NENA i3 Standard for Next Generation 9-1-1*.[4]
[Ref 15] ATIS-0500032, *ATIS Standard for Implementation of an IMS-based NG9-1-1 Service Architecture*. [2]

# 3 Definitions, Acronyms, & Abbreviations

For a list of common communications terms and definitions, please visit the *ATIS Telecom Glossary*, which is located at < http://www.atis.org/glossary >.

## *3.1 Definitions*

**Caller ID**: The originating or calling party telephone number used to identify the caller.

**Emergency Call:** A generic term used to include any type of Request For Emergency Assistance (RFEA). In North America, the 3-digit code “9-1-1” is typically used to facilitate the reporting of an emergency requiring response by a Public Safety agency.

## *3.2 Acronyms & Abbreviations*

| | |
|---|---|
| 3GPP | Third Generation Partnership Project |
| ADR | Additional Data Repository |
| ALI | Automatic Location Identification |
| ANI | Automatic Number Identification |
| ASCII | American Standard Code for Information Interchange |
| ATIS | Alliance for Telecommunications Industry Solutions |
| BCF | Border Control Function |
| BGCF | Breakout Gateway Control Function |
| CAMA | Centralized Automatic Message Accounting |
| COS | Class of Service |
| CPE | Customer Premises Equipment |
| E9-1-1 | Enhanced 9-1-1 |

[4] This document is available from NENA: The 9-1-1 Association at: < https://www.nena.org >.

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

[6] This document is available from the International Telecommunication Union (ITU) at: < https://www.itu.int/ >.

| | |
|---|---|
| ECRF | Emergency Call Routing Function |
| E-CSCF | Emergency Call Session Control Function |
| E-MF | Enhanced Multi-Frequency |
| ESIF | Emergency Services Interconnection Forum |
| ESInet | Emergency Services IP Network |
| ELT | English Language Translation |
| ESGW | Emergency Services Gateway |
| ESN | Emergency Service Number |
| EMS | Emergency Medical Service |
| ESRD | Emergency Services Routing Digits |
| ESQK | Emergency Services Query Key |
| ESRK | Emergency Services Routing Key |
| ESRP | Emergency Service Routing Proxy |
| FCC | Federal Communications Commission |
| GMLC | Gateway Mobile Location Center |
| HTTPS | HyperText Transfer Protocol Secure |
| IAM | Initial Address Message |
| IBCF | Interconnection Border Control Function |
| IMS | IP Multimedia Subsystem |
| IP | Internet Protocol |
| ISUP | Integrated Services Digital Network User Part |
| ITU-T | International Telecommunication Union Telecommunication Standardization Sector |
| JSON | JavaScript Object Notation |
| JWT | JSON Web Token |
| LBR | Location-Based Routing |
| LIS | Location Information Server |
| LNG | Legacy Network Gateway |
| LPG | Legacy PSAP Gateway |
| LRF | Location Retrieval Function |
| LS | Location Server |
| LSRG | Legacy Selective Router Gateway |
| MF | Multi-Frequency |
| MGCF | Media Gateway Control Function |
| MLP | Mobile Location Protocol |
| MLTS | Multi-Line Telephone Systems |
| MPC | Mobile Positioning Center |
| MSC | Mobile Switching Center |
| NANP | North American Numbering Plan |
| NCAS | Non-Call Associated Signaling |
| NENA | National Emergency Number Association |
| NG | Next Generation |
| NG9-1-1 | Next Generation 9-1-1 |
| NPA | Numbering Plan Area |
| NPD | Numbering Plan Digit |

| | |
|---|---|
| OCIF | Outbound Call Interface Function |
| OOB | Out-of-Band |
| OSP | Originating Service Provider |
| pANI | Pseudo ANI |
| PASSporT | Personal Assertion Token |
| P-CSCF | Proxy Call Session Control Function |
| PTSC | Packet Technologies and Systems Committee |
| PSAP | Public Safety Answering Point |
| RDF | Routing Determination Function |
| RFEA | Request For Emergency Assistance |
| RPH | Resource-Priority Header |
| SHAKEN | Signature-based Handling of Asserted information using toKENs |
| S-CSCF | Serving Call Session Control Function |
| SIP | Session Initiation Protocol |
| SKS | Secure Key Store |
| SR | Selective Router |
| SRDB | Selective Routing Database |
| SS7 | Signaling System No. 7 |
| STI | Secure Telephone Identity |
| STI-AS | Secure Telephone Identity Authentication Service |
| STI-CPS | Secure Telephone Identity Call Placement Service |
| STI-CR | Secure Telephone Identity Certificate Repository |
| STI-IWF | Secure Telephone Identity Interworking Function |
| STI-OOBS | Secure Telephone Identity Out-of-Band Service |
| STIR | Secure Telephone Identity Revisited |
| STI-VS | Secure Telephone Identity Verification Service |
| TDM | Time Division Multiplexing |
| TG | Trunk Group |
| TSP | Terminating Service Provider |
| UE | User Equipment |
| URI | Uniform Resource Identifier |
| URL | Uniform Resource Locator |
| URN | Uniform Resource Name |
| UUI | User-to-User Information |
| WCM | Wireline Compatibility Mode |
| WSP | Wireless Service Provider |
| WTSC | Wireless Technologies and Systems Committee |

# 4 Description of Non-IP Call Authentication Solutions

ATIS formed the Non-IP Call Authentication Task Force under the Packet Technologies and Systems Committee (PTSC) to identify and document call authentication challenges facing Time Division Multiplexing (TDM) networks, investigate the feasibility of potential solutions in this area, and evaluate the viability of implementing TDM call authentication frameworks. The Non-IP Call Authentication Task Force has been considering three alternative mechanisms for supporting caller authentication in scenarios where end-to-end SIP is not available. This includes scenarios where the Originating Service Provider (OSP) supports a TDM network, the Terminating Service Provider (TSP) supports a TDM network, or one or more TDM transport links or transit networks are used to interconnect an OSP and TSP. The alternative approaches for caller authentication in TDM networks under consideration by the Non-IP Call Authentication Task Force include:

- SHAKEN Out-of-Band (OOB) PASSporT Transmission Involving TDM Networks
- Extending STIR/SHAKEN Over TDM
- PASSporT Encoded in Integrated Services Digital Network User Part (ISUP) User-to-User Information (UUI) Parameter[7]

## *4.1 SHAKEN OOB PASSporT Transmission Involving TDM Networks*

As described in ATIS-1000096 [Ref 2], *Signature-Based Handling of Asserted Information Using Tokens (SHAKEN): Out-of-Band PASSporT Transmission Involving TDM Networks* [Ref 2], this caller authentication mechanism extends the currently defined SHAKEN framework to enable the transmission of Personal Assertion Tokens (PASSporTs) for calls that are originated and/or terminated by TDM service providers and for calls that use TDM-based interconnections or transit networks. The SHAKEN Out-of-Band (OOB) PASSporT Transmission Involving TDM Networks mechanism allows cryptographically signed “shaken” PASSporTs to be exchanged between TDM networks out-of-band (i.e., outside of the telephone network signaling). The out-of-band exchange of PASSporTs is based on *Out-of-Band STIR for Service Providers* [draft-ietf-stir-servprovider-oob) [Ref 3]. The SHAKEN OOB PASSporT Transmission Involving TDM Networks call authentication mechanism assumes that, at a minimum, TDM networks are Signaling System No. 7 (SS7)-capable. It also requires support for new functional elements and interfaces in TDM networks.

One such functional element is the Secure Telephone Identity Call Placement Service (STI-CPS). The STI-CPS is used by TDM service providers to exchange PASSporTs. In the context of this caller authentication mechanism, the STI-CPS receives PASSporTs from a TDM originating network or from an originating or transit network that is performing SIP-to-TDM interworking, and supports retrieval of the PASSporTs by the destination network or a transit network that is performing TDM-to-SIP interworking. An STI-CPS has a standardized interface over which service providers can publish and retrieve PASSporTs. Using this call authentication mechanism, if a call originates in a SIP network and is passed to a transit service provider who sends the call over a TDM interconnection to a downstream TDM network, the transit service provider is responsible for publishing the PASSporT(s) received in the SIP signaling to the STI-CPS, since the PASSporT(s) it receives in a SIP INVITE message will be lost in the conversion to TDM. Similarly, when an OSP originates a call via SIP but then sends the call to a transit service provider over a TDM interconnection, the OSP must generate the applicable PASSporT(s) and publish the PASSporT(s) to an STI-CPS before forwarding the call over the TDM interconnection.

Conversely, a transit service provider who receives a call from an upstream TDM network and sends the call to a downstream SIP network is responsible for retrieving the PASSporT(s) from the STI-CPS and restoring in-band transmission of the PASSporT(s) in outgoing SIP signaling. Additionally, a service provider that retrieves one or more PASSporTs must reconstruct any SIP headers that were lost in the conversion from SIP to TDM and back to SIP, and that are protected by the PASSporTs. Similarly, if a TSP receives the call from a transit service provider via TDM, then the TSP is responsible for retrieving the PASSporT(s) from the STI-CPS so that STIR/SHAKEN verification functions can be performed by the terminating network.

[7] Note that this alternative is being documented as an extension to the Extending STIR/SHAKEN Over TDM mechanism documented in ATIS-1000095 [Ref 4]. This Technical Report analyzes these mechanisms separately.

An STI-CPS is expected to re-publish all of the PASSporTs it receives to every other STI-CPS within the SHAKEN ecosystem. This allows service providers to retrieve PASSporT(s) from any STI-CPS, regardless of which STI-CPS the PASSporT was originally published to, without having to support an STI-CPS discovery mechanism.

In addition to the STI-CPS, the architecture to support the SHAKEN OOB PASSporT Transmission Involving TDM Networks caller authentication mechanism also includes a Secure Telephone Identity Out-of-Band Service (STI-OOBS) functional element. The STI-OOBS interacts directly with the STI-CPS to publish PASSporTs to, and retrieve PASSporTs from, an STI-CPS. The STI-OOBS supports a SIP interface to receive INVITE messages that contain one or more PASSporTs and uses a HyperText Transfer Protocol Secure (HTTPS) interface to publish those PASSporTs, along with a JSON Web Token (JWT) for authentication, to an STI-CPS. If the STI-OOBS receives an INVITE that does not contain any PASSporTs (as would be the case for a TDM terminating network or a SIP terminating network that receives the call from a TDM transit network), the STI-OOBS constructs a JWT for authentication, retrieves any available PASSporTs from an STI-CPS that have the same calling and called party information as is included in the retrieval request, and includes the retrieved PASSporTs in the SIP response.

For calls that originate from, or terminate to, a TDM network, the architecture supporting this caller authentication mechanism also includes a Secure Telephone Identity Interworking Function (STI-IWF) that is responsible for performing SS7-SIP interworking, as well as other SHAKEN-specific functionality. If the originating network is a TDM network, then in addition to performing SS7-SIP interworking, the STI-IWF will interact with a Secure Telephone Identity Authentication Service (STI-AS) for SHAKEN authentication and to obtain any associated PASSporTs. The STI-IWF is then responsible for interacting with the STI-OOBS so that the PASSporT(s) can be published to the STI-CPS. The STI-IWF is also responsible for returning SS7 signaling to the TDM switch that will allow call processing/routing to proceed.

If the terminating network is a TDM network, it will invoke STI-IWF functionality to support SS7-SIP interworking as well as SHAKEN-specific functionality which includes interacting with an STI-OOBS to obtain any PASSporTs that are associated with the call. After receiving the PASSporT(s) from the STI-OOBS, the STI-IWF in the terminating TDM network will interact with a SHAKEN Secure Telephone Identity Verification Service (STI-VS) for verification of the PASSporT(s). The mechanism for returning verification status obtained by the STI-IWF to TDM switch for use by the TSP is left to implementation.

Clause 8 of ATIS-1000096 [Ref 2] describes a number of example call scenarios using the SHAKEN OOB PASSporT Transmission Involving TDM Networks mechanism. A subset of these call scenarios, which are relevant to the discussion of caller authentication in an E9-1-1 or Transitional NG9-1-1 environment, are re-created below.

Figure 4-1 illustrates how the OOB PASSporT Transmission Involving TDM Networks mechanism could be applied in an end-to-end TDM call scenario.

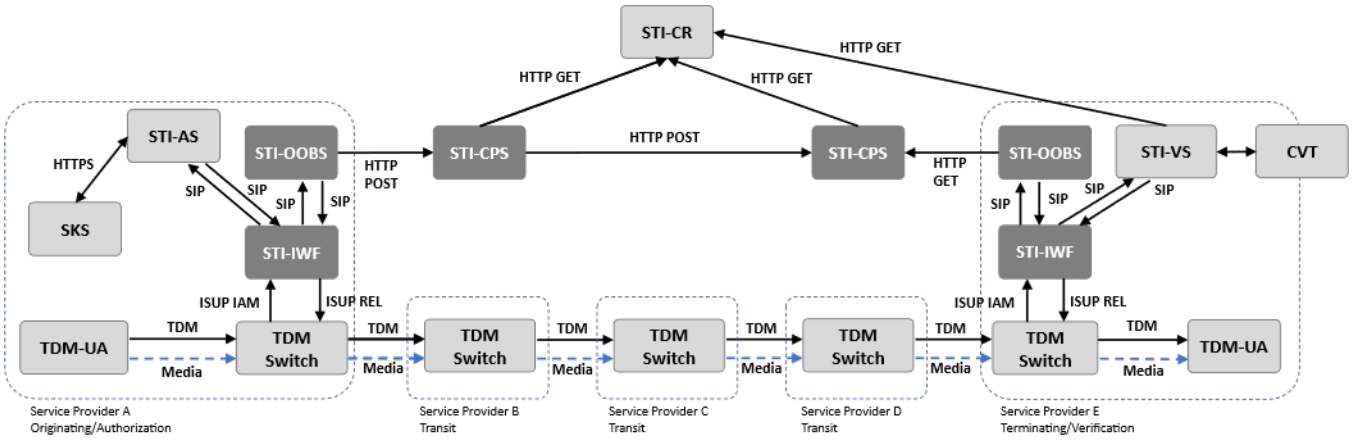



**Figure 4.1: End-to-End TDM**

The sequence illustrated by this call flow example is as follows:

1. The call originates in a TDM network (Service Provider A).
2. An SS7 Initial Address Message (IAM) is forwarded by the TDM switch to the STI-IWF.
3. The STI-IWF performs SS7-SIP interworking then sends the resulting SIP INVITE message to the STI-AS for SHAKEN authentication and to obtain the associated PASSporT(s).
4. Upon receiving the INVITE containing the signed PASSporT(s) from the STI-AS, the STI-IWF forwards the SIP INVITE to the STI-OOBS.
5. The STI-OOBS publishes the PASSporT(s) to the STI-CPS, which publishes the PASSporT(s) to all of the other STI-CPSs.
6. The SIP-OOBS also returns a SIP 503 Service Unavailable message to the STI-IWF.
7. The STI-IWF returns an SS7 RELEASE message with cause code 34 (no circuit available) to the TDM switch.
8. The TDM switch route advances to select the route used to progress the call.
9. Service Provider A then delivers the call downstream via TDM transit networks to a TDM terminating network (Service Provider E).
10. The terminating network (Service Provider E) also supports an STI-IWF that performs SS7-SIP interworking and interacts with the STI-OOBS to obtain the PASSporT(s) for the call.
11. The STI-IWF then interacts with the SHAKEN STI-VS for verification of the PASSporT(s).

Subsequent processing by the terminating network is left to implementation.

Figure 4-2 illustrates how the OOB PASSporT Transmission for TDM Networks mechanism could be applied in a scenario where a call originates in a SIP network, transits SIP and TDM-based transit networks, and terminates in a TDM terminating network.

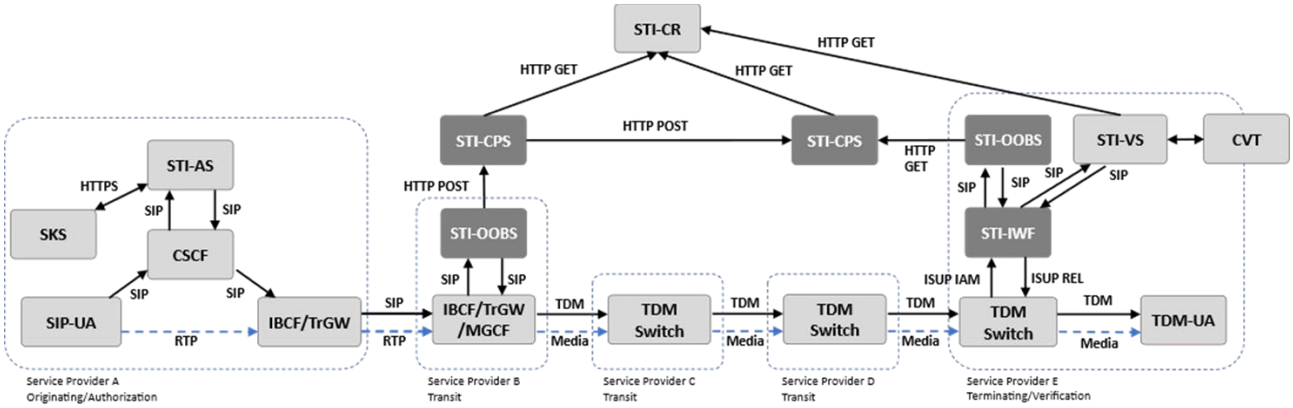



**Figure 4.2: SIP Originating Network, TDM Terminating Network, SIP and TDM Transit Networks**

The sequence illustrated by this call flow example is as follows:

1. The call originates in a SIP (Service Provider A) network and is authenticated using SHAKEN.
2. Service Provider A interconnects with a transit network provider (Service Provider B) via SIP; the SIP INVITE message passed from originating Service Provider A to transit Service Provider B contains the signed PASSporT(s) obtained from the STI-AS.
3. Service Provider B is responsible for publishing the PASSporT(s) to the STI-CPS by passing the SIP INVITE message containing the PASSporT information to the STI-OOBS,
4. Service Provider B also performs SIP-SS7 interworking and sends the call downstream over a TDM/SS7 trunk.

5. The terminating network (Service Provider E) receives the call from transit Service Provider D via a TDM/SS7 interconnection and is responsible for retrieving the PASSporT(s) from the STI-CPS by passing the SS7 IAM to the STI-IWF.
6. The STI-IWF interworks the SS7 IAM to a SIP INVITE and passes the SIP INVITE to the STI-OOBS.
7. The STI-OOBS interacts with the STI-CPS to retrieve the PASSporT(s) and returns a SIP INVITE with the PASSporT(s) to the STI-IWF.
8. The STI-IWF interacts with the STI-VS to verify the PASSporT(s).

Subsequent processing by the terminating TDM network is left to implementation.

Figure 4-3 illustrates how the OOB PASSporT Transmission for TDM Networks mechanism could be applied in a scenario where a call originates in a TDM network, terminates in a SIP network and transits TDM and SIP transit networks.

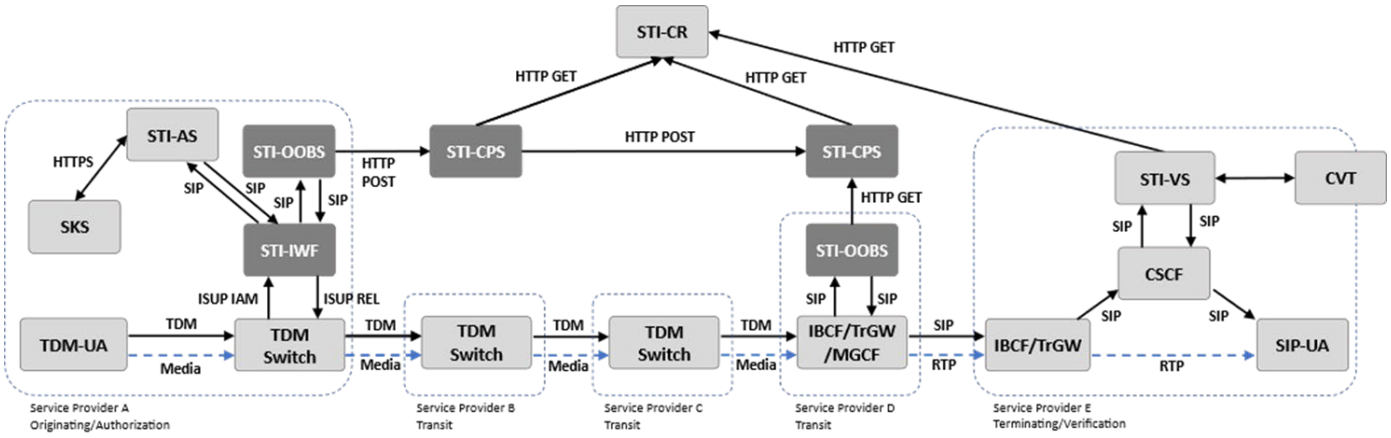



**Figure 4.3: TDM Originating Network, SIP Terminating Network, TDM and SIP Transit Networks**

The sequence illustrated by this call flow example is as follows:

1. The call originates in a TDM network (Service Provider A).
2. An SS7 Initial Address Message is forwarded by the TDM switch to the STI-IWF.
3. The STI-IWF performs SS7-SIP interworking then sends the resulting SIP INVITE message to the STI-AS for SHAKEN authentication and to obtain the associated PASSporT(s).
4. Upon receiving the INVITE containing the signed PASSporT(s) from the STI-AS, the STI-IWF forwards the SIP INVITE to the STI-OOBS.
5. The STI-OOBS publishes the PASSporT(s) to the STI-CPS, which publishes the PASSporT(s) to all of the other STI-CPSs.
6. The SIP-OOBS also returns a SIP 503 Service Unavailable message to the STI-IWF.
7. The STI-IWF returns an SS7 RELEASE message with cause code 34 (no circuit available) to the TDM switch.
8. The TDM switch route advances to select the route used to progress the call.
9. The last transit service provider (Service Provider D) receives the call via an upstream TDM interconnection.
10. Service Provider D is responsible for retrieving the PASSporT(s) from the STI-CPS by interworking the incoming SS7 signaling to SIP and forwarding the SIP INVITE message to the STI-OOBS.
11. The STI-OOBS generates a JWT and sends a retrieval request containing the calling and called information associated with the call to the STI-CPS.
12. The STI-CPS returns the PASSporT(s) to the STI-OOBS.
13. The STI-OOBS populates the PASSporT information in the SIP INVITE message and returns it to the interworking/gateway functionality in Service Provider D's network.

14. Service Provider D then sends the SIP INVITE containing the PASSporT information to the terminating network (Service Provider E) via a SIP interconnection.
15. The terminating network (Service Provider E) performs SHAKEN verification.

## *4.2 Extending STIR/SHAKEN over TDM*

ATIS-1000095, *Extending STIR/SHAKEN over TDM* [Ref 4], describes a caller authentication mechanism that extends the SHAKEN framework to enable the conveyance of verified attestation levels associated with calls that originate in, terminate to, or transit TDM networks. This approach assumes that SS7 ISUP signaling is used over the TDM portions of the call path. It relies on bilateral agreements and transitive trust between operators on each end of a direct TDM connection. The nature of the agreement, or whether there is an agreement at all, is determined on a per-TDM connection basis. The same mechanism can be used among several operators as long as they all agree to do so.

This caller authentication solution supports two different ways of conveying verified attestation levels (i.e., attestation level “A”, “B”, or “C”, as well as indicating that no Identity header was received) over TDM networks. Interconnected network providers may also agree to only signal a subset of the values, e.g., attestation level “A” and “no Identity header received”.

The first model uses certain values (or spare values) of ISUP parameters to signal attestation level and verification status information. ATIS-1000095 [Ref 4] describes the use of the ISUP Screening Indicator in the Calling Party Number parameter for this purpose, although it acknowledges that other parameters could be used, such as spare bits in the second octet of the Called Party Parameter, spare bits of the Call Reference etc. The critical aspect of this solution is that the two ends of the TDM interconnection agree on which parameters are used and how to interpret the values that are populated.

The second model uses different trunk groups (TGs) to convey different attestation level values. For example, TG-1 could be used for “No Identity header received”, TG-2 for “A”, TG-3 for “B” and TG-4 for “C”.

Using the Extending STIR/SHAKEN over TDM approach, a SIP/SHAKEN-capable terminating network that receives a call where an Identity header is present in the incoming signaling will use normal SHAKEN procedures to verify the Identity header in the incoming SIP INVITE message. If a SIP/SHAKEN-capable transit network receives a call where an Identity header is present, and the next network in the call path is interconnected via TDM/SS7 trunks, the transit network will use normal SHAKEN procedures to verify the Identity header, and if the Identity header validates successfully, will signal the verified attestation value over the TDM interconnection based on the model agreed to by the operator at the other end of TDM interconnection. If a SIP/SHAKEN-capable network receives a call via a TDM interconnection, and the call is subsequently routed over a SIP interconnection, the operator of the transit network will generate a new Identity header with the attestation level it received over the TDM interconnection, and use its own private key (i.e., Secure Telephone Identity [STI] certificate) to generate a new PASSporT for inclusion in the outgoing SIP signaling.

The Extending STIR/SHAKEN over TDM caller authentication mechanism defines mappings using the ISUP Screening Indicator for the following topologies: “TDM Interconnect”; “TDM Termination”; and “TDM Origination”.

“TDM Interconnect”, as described in ATIS-1000095 [Ref 4], refers to the scenario where TDM is used to connect two SIP islands. It is illustrated in Figure 4-4.

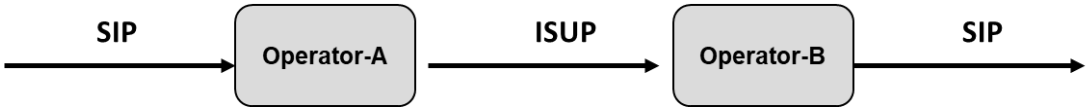



**Figure 4.4: TDM Interconnect Topology**

ATIS-1000095 [Ref 4] describes the following mapping between verified attestation levels and ISUP Screening Indicator values as applicable to the TDM Interconnect topology. This would be populated by Operator-A.[8]

| Attestation Level | Verification Status | Screening Indicator |
|---|---|---|
| A | Passed | 11 – network provided |
| B | Passed | 00 – user provided, not verified |
| C | Passed | 00 - user provided, not verified |
| Any | Failed | 10 - user provided, verified and failed |
| No Identity | <no verification> | 00 - user provided, not verified |

To support the outgoing SIP signaling from Operator-B, ATIS-1000095 [Ref 4] describes the following mapping from the ISUP Screening Indicator values received from Operator-A to an Identity header or to a verstat (if an Identity header is not to be further propagated).

| Screening Indicator | Identity header generated with Attestation Level | verstat |
|---|---|---|
| 01 - user provided, verified and passed<br>(01 is not used for Identity to Screening Indicator mapping for interconnect scenarios per the mapping defined in this document. It may be used by an ATIS-1000679 [Ref 5] compliant entity or by an entity in TDM domain) | A | TN-Validation-Passed |
| 10 - user provided, verified and failed | No Identity header | TN-Validation-Failed |
| 11 - network provided | A | TN-Validation-Passed |
| 00 - user provided, not verified | B/C or No Identity header based on policy | No-TN-Validation or not included based on policy |

NOTE: It is important that the Screening Indicator be monitored at network ingress points and changed to “user provided, not verified” if the call is coming from a network that does not adhere to this use of this parameter as described in ATIS-1000095 [Ref 4].

The “TDM Termination” topology is defined as a scenario where TDM is used in the TSP network. The topology diagram associated with this call scenario is illustrated in Figure 4-5.

[8] Note that ATIS-1000095 [Ref 4] uses Screening Indicator values as defined in ITU-T Recommendation Q.763 (12/1999) [Ref 11]. Based on ATIS-1000113.2015 [Ref 12], the Screening Indicator value “01” corresponds to “user provided, screening passed”, value “00” corresponds to “user provided, not screened”, and value “10” corresponds to “user provided, screening failed”.

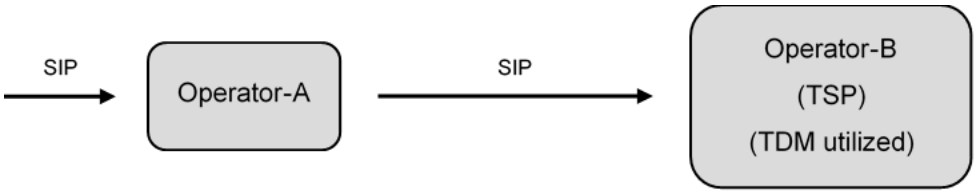



**Figure 4.5: TDM Termination Topology**

In the context of the TDM termination topology, ATIS-1000095 [Ref 4] describes the following mappings from attestation level and verification status to ISUP Screening Indicator values. This would be populated by Operator-B.

| Attestation Level | Verification Status | Screening Indicator |
|---|---|---|
| A | Passed | 11 – network provided |
| B | Passed | 00 – user provided, not verified |
| C | Passed | 00 - user provided, not verified |
| Any | Failed | 10 - user provided, verified and failed |
| No Identity | <no verification> | 00 - user provided, not verified |

Since the TDM network is the terminating network, no mapping from the ISUP Screening Indicator to the Identity header/attestation level or to the verstat is needed.

The “TDM Origination” topology is defined in ATIS-1000095 [Ref 4] as a scenario where TDM is used in the OSP network. The topology diagram associated with this call scenario is illustrated in Figure 4-6.

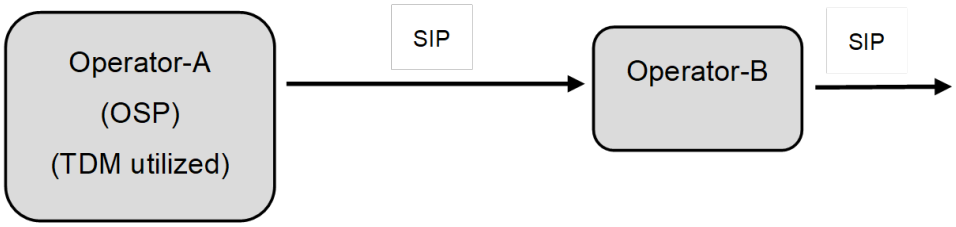



**Figure 4.6: TDM Origination Topology**

In the context of the TDM origination call scenario, ATIS-1000095 [Ref 4] defines the following mapping between ISUP Screening Indicator values and attestation level/verstat. This would be populated by Operator-A.

| Screening Indicator | Attestation Level | Verstat |
|---|---|---|
| 01 - user provided, verified and passed | A | TN-Validation-Passed |
| 10 - user provided, verified and failed | No Identity header | TN-Validation-Failed |
| 11 - network provided | A | TN-Validation-Passed |
| 00 - user provided, not verified | B/C or No Identity header based on policy | No-TN-Validation or not included based on policy |

In this scenario, and in the “TDM Interconnect” scenario, it would also be possible to use TG information to populate the SIP Identity Header or to set the ISUP Screening Indicator for conversion to a SIP Identity header by a downstream element.

ATIS-1000095 [Ref 4] is structured to take advantage of existing ISUP signaling parameters to minimize the impact on existing TDM switches. It uses TDM switch provisioning and configuration capabilities, where possible, to identify and communicate attestation levels to the terminating service provider over TDM interconnects. As a result, this mechanism provides a degree of call authentication (i.e., attestation level) for TDM switches with TDM interconnects while minimizing the impact on existing TDM equipment.

## *4.3 PASSporT Encoded in ISUP User-to-User Information (UUI) Parameter*

A third non-IP call authentication alternative being discussed by the ATIS Non-IP Call Authentication Task Force proposes encoding a Secure Telephone Identity (STI) PASSporT within an ISUP UUI parameter. This mechanism is being viewed as an extension to the Extending STIR/SHAKEN over TDM mechanism. This mechanism proposes the use of an SS7 signaling parameter to convey PASSporTs in architectures that involve TDM interconnections. Specifically, this mechanism proposes that a single STI PASSporT be encoded in the SS7 ISUP UUI parameter when converting from SIP to TDM. When converting from TDM to SIP, the UUI is used to (re)construct the STI PASSporT in the Identity header of the outgoing SIP message. Since discussions related to this mechanism are ongoing, the material in this clause is subject to change.

One consideration related to the use of the UUI parameter to convey an STI PASSporT is the maximum size of the UUI parameter. Since the UUI parameter is currently defined to have a length of between 3 and 131 octets, there is concern that encoding a PASSporT in the UUI may exceed the length allowed for the UUI parameter, or that inclusion of the PASSporT in the UUI will cause the maximum length of the SS7 IAM (i.e., 272 bytes) to be exceeded. If the maximum length of the IAM is exceeded, message segmentation will be necessary. Since segmentation of IAMs is not widely implemented, this non-IP call authentication solution should not be used if it requires segmentation of SS7 IAMs. As a result, the following criteria have been established that limit the use of this mechanism to SIP-to-ISUP interworking scenarios where: (1) the ISUP UUI is not used for any other purpose; (2) the encoded PASSporT size is less than 129 bytes; and (3) the encoded PASSporT size does not cause ISUP IAM message size to exceed 232 bytes. In addition, there needs to be alignment in the mappings between SIP headers and ISUP parameters (when interworking from SIP to ISUP and from ISUP to SIP) for those SIP headers/ISUP parameters that are associated with claims that are relevant to the PASSporT but encoded in the UUI; otherwise, the claims in the PASSporT won’t match the SIP headers generated as a result of applying ISUP-to-SIP interworking. In addition to the criteria described above, there are other constraints related to privacy of the caller identity information that are not applicable to 9-1-1 calls.

With SS7 parameter/message length considerations in mind, an objective of this non-IP call authentication mechanism is to use encoding schemes that will allow an STI PASSporT to be conveyed in a UUI parameter using the least number of bytes. To minimize the size of the PASSporT information, proposals have focused on reducing the size of the “x5u” parameter in the PASSporT header. The “x5u” parameter contains the Uniform Resource Locator (URL) associated with the certificate repository that contains the X.509 public key certificate that was used to sign the PASSporT.

An entity performing SIP-to-ISUP interworking must check to see whether the criteria described above for embedding an STI PASSporT in a UUI are met. Whether or not the criteria are met, the interworking entity will

populate the Screening Indicator using the mechanisms described in Clause 4.2 of this document if there is a bilateral agreement to use it for conveyance of SHAKEN attestation level.

An entity performing ISUP-to-SIP interworking will examine the first byte of the UUI to determine whether it contains the value “01001010”, which indicates that an STI PASSporT is encoded in the UUI. The interworking entity will also check to see that the Issued At (“iat”) date is within the acceptable date/time range, and that the UUI size is consistent with the expected value. Assuming the above checks are successful, the interworking entity will then send a request to verify the signature in the PASSporT.

A SIP INVITE may contain a “shaken” PASSporT with optional claims or may contain other PASSporTs (e.g., an “rph” PASSporT). The PASSporT Encoded in ISUP UUI mechanism supports the transfer of attestation information associated with PASSporTs other than “shaken” PASSporTs over the TDM domain in a cryptographically secure manner using the following optional procedures. Note that these procedures will only apply to PASSporTs that are supported by the SIP-to-ISUP interworking entity. If the SIP-to-ISUP interworking entity receives multiple claims in a single PASSporT, then the original PASSporT will be encoded in ISUP UUI parameter, and the original signature is maintained. If the SIP-to-ISUP interworking entity receives claims in multiple PASSporTs, then it will generate a new PASSporT in the form of a “shaken” PASSporT that includes all of the claims from the received PASSporTs. The interworking entity will then encode this new PASSporT in an ISUP UUI parameter. A new signature will be generated and used with the private key of the entity performing this operation.

Of particular interest, in the context of 9-1-1, are the procedures related to the handling of “rph” PASSporTs, since SIP signaling associated with a 9-1-1 call will include a Resource-Priority header. Since there is no canonical approach to interworking “rph” claims into ISUP parameters and then back to “rph” claims, the approach that encodes an STI PASSporT in an ISUP UUI describes a mechanism that encodes “rph” claims (and an “sph” claim associated with an emergency callback, if a Priority header set to “psap-callback” is received in the incoming SIP signaling) in dedicated fields in the ISUP UUI parameter. Due to ISUP IAM/ISUP UUI parameter size limitations, more than one PASSporT cannot be encoded in a UUI. If an “rph” PASSporT is received in incoming SIP signaling along with a “shaken” PASSporT, the SIP-to-ISUP interworking entity will generate a new “shaken” PASSporT with “rph” claims and sign it.

At an ISUP-to-SIP interworking point, the signature received in the ISUP UUI is verified. Additional processing is only applied if verification is successful. A SHAKEN PASSporT is generated based on the ISUP UUI parameter content. An ISUP-to-SIP interworking entity will not use the “rph” claims present in an ISUP UUI to generate “rph” claims in an “rph” PASSporT unless regulatory rules allow it (e.g., an “rph” PASSporT may only be generated if the interworking entity has authority over the relevant namespaces).

This non-IP call authentication mechanism is intended to be used for calls that originate in a SIP network, traverse a TDM network, and terminate in a SIP network. While it is technically possible for a call originating in a TDM network to utilize this mechanism, enhancements would be needed to support SHAKEN functionality to allow the legacy network to generate an STI PASSporT and encode it in a UUI according to the specified rules. Such enhancements are not considered practical for legacy networks. Calls terminating to a TDM network may use the Screening Indicator-based mechanism described in Clause 4.2.

# 5 Description of Emergency Services Architectures

## *5.1 E9-1-1 Architectures*

A unique feature of E9-1-1 is Selective Routing. Selective Routing allows 9-1-1 calls to be routed to the appropriate PSAP based on the calling number/Automatic Number Identification (ANI), or other location information that may be provided with the call. A Selective Router (SR) is a specially equipped TDM switch that controls the delivery of voice calls to PSAPs with ANI information. To support Selective Routing, an SR interacts with a Selective Routing Database (SRDB) by providing the calling number/ANI or location key to the SRDB and having the SRDB return an Emergency Service Number (ESN)[9] that is used to identify the path to the target PSAP for the emergency call. In addition to Selective Routing, an SR supports other 9-1-1-related feature functionality including transfer and speed calling. In an E9-1-1 environment, an SR typically receives emergency calls over dedicated Multi-Frequency (MF) or SS7-supported trunk groups from wireline end offices and Mobile Switching Centers (MSCs). As described

[9] An ESN may also play a role in selecting the transfer-to PSAP if the primary PSAP requests selective transfer of the emergency call and identifying English Language Translations (ELTs) that specify the corresponding police, fire, and Emergency Medical Service (EMS).

above, the SR uses information it receives in incoming signaling to identify the PSAP that serves the area in which the call originated. Emergency calls are typically delivered by the SR to a PSAP over traditional Centralized Automatic Message Accounting (CAMA)-like (i.e., Traditional Multi-Frequency [MF]) or Enhanced MF (E-MF) interfaces. Traditional MF supports the delivery of a 7-digit number, along with a single Numbering Plan Digit (NPD) that can be used to derive the Numbering Plan Area (NPA) and to indicate whether the ANI information should be displayed using a steady or flashing display.[10] E-MF is a Feature Group D-like signaling scheme that is more commonly used between SRs and PSAPs. E-MF supports the delivery of either one or two 10-digit numbers to the PSAP with the call, along with an ANI II value that tells the PSAP Customer Premises Equipment (CPE) whether to display the information using a steady or flashing display. The MF signaling delivered to a PSAP includes a key that the PSAP will use to query an Automatic Location Identification (ALI) system for caller location information. This location information can be used to support the dispatch of emergency personnel to an incident.

When a wireline caller originates an emergency call, the call is routed from the caller's serving end office, over a (typically dedicated) MF or SS7 trunk group, to an SR. The signaling associated with the 9-1-1 call will include the caller's telephone number signaled as an MF ANI or in an SS7 Calling Party Number parameter. After determining the target PSAP for the call (by querying an SRDB using the ANI/calling party number), the SR delivers the call along with the telephone number to the PSAP over a Traditional MF or E-MF interface, as appropriate for the PSAP. The PSAP then uses that telephone number to query an ALI system for location information. In the case of wireline emergency callers, the ALI database contains static telephone number-to-street address mappings. Figure 5-1 provides a representative architecture for wireline E9-1-1.

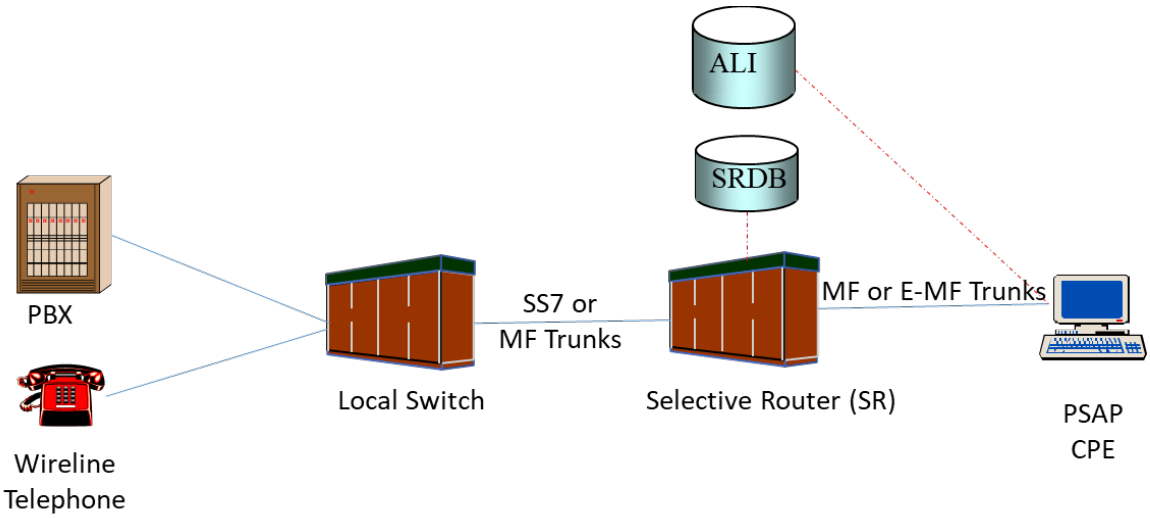



**Figure 5.1: E9-1-1 Architecture for Wireline Emergency Calls**

Enhanced wireless emergency services (i.e., wireless E9-1-1), requiring wireless carriers to provide the location of the wireless 9-1-1 callers to PSAPs, is mandated by the FCC. In the context of wireless E9-1-1, a Mobile Switching Center (MSC) provides emergency call-related information to an SR using SS7 or Feature Group-D MF signaling. Wireless E9-1-1 calls are delivered by the SR to a PSAP using the same Traditional MF or E-MF interfaces as for wireline E9-1-1. If the E-MF interface to the PSAP supports the delivery of two 10-digit numbers, the PSAP may receive a callback number as well as a pseudo-ANI (pANI) (i.e., a location key) with an emergency call. The PSAP will use the callback number and/or the pANI (depending on implementation) to query the ALI system.

To fulfill regulatory requirements with regard to the delivery of latitude and longitude associated with a 9-1-1 call, wireless carriers have deployed location determination technology in their networks. However, due to limitations in today's location determination technology resulting in delays in obtaining Phase II location, implementations typically support the delivery of a location key in the call setup signaling, with Phase II location information delivered over a separate data link between the wireless network and the emergency services network. When an ALI system

[10] A flashing display is intended to alert the PSAP call-taker of special conditions related to call treatment.

receives an ALI request from a PSAP, the ALI system will query a Mobile Positioning Center (MPC) in the wireless network, typically using the E2 protocol.[11] The E2 protocol defined in J-STD-036-C-2 [Ref 13] and NENA-STA-018.2-2021 (originally NENA 05-001) [Ref 8] can be used to obtain initial caller location information as well as updated location information, when requested.

J-STD-036-C-2 [Ref 13] defines two methods for delivering Phase II location from the wireless network to the emergency services network via a separate data link. One is referred to as the Non-Call Associated Signaling (NCAS) approach, and the other is referred to as the Wireline Compatibility Mode (WCM) approach. Of the two variants, the WCM approach is more widely deployed.

With the wireless NCAS approach, the MSC sends a callback number and the cell site identifier (represented by Emergency Services Routing Digits [ESRD]) to the SR using either MF or SS7 signaling. The SR uses the ESRD to interact with the SRDB, and the SRDB returns routing information associated with the target PSAP. The interface between the SR and the PSAP will typically be an E-MF interface that supports the delivery of both the callback number and the ESRD to the PSAP, although hybrid arrangements (involving the real-time update of the ALI data via the SR) may be used if the PSAP supports either a Traditional MF interface or the delivery of a single 10-digit number via an E-MF interface. Figure 5-2 illustrates wireless emergency call handling using the NCAS approach.

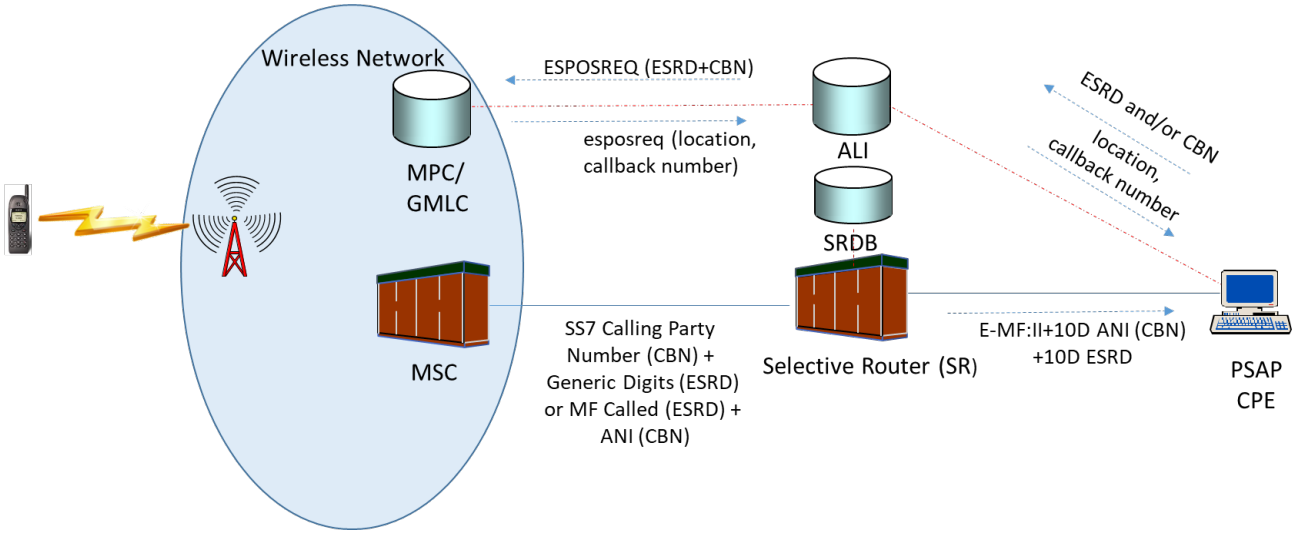



**Figure 5.2: Wireless E9-1-1 – NCAS Approach**

With the WCM approach, as defined in J-STD-036-C-2 [Ref 13], only an Emergency Services Routing Key (ESRK) is signaled with the call. All of the location information, as well as the callback number, are sent over a separate data link to the ALI database from the wireless network. The MSC delivers a single 10-digit number (i.e., the ESRK) to the SR, and the SR delivers a single 7/10-digit number to the PSAP. The ESRK represents the PSAP and uniquely identifies the 9-1-1 call. The ESRK also identifies the MPC/GMLC in the wireless network that the ALI system must query to acquire location information for the call. Figure 5-3 illustrates wireless emergency call handling using the WCM approach.

[11] Some implementations use the Mobile Location Protocol (MLP) to support interactions between the ALI system and an MPC/Gateway Mobile Location Center (GMLC) in the wireless network to obtain the location associated with an emergency call.

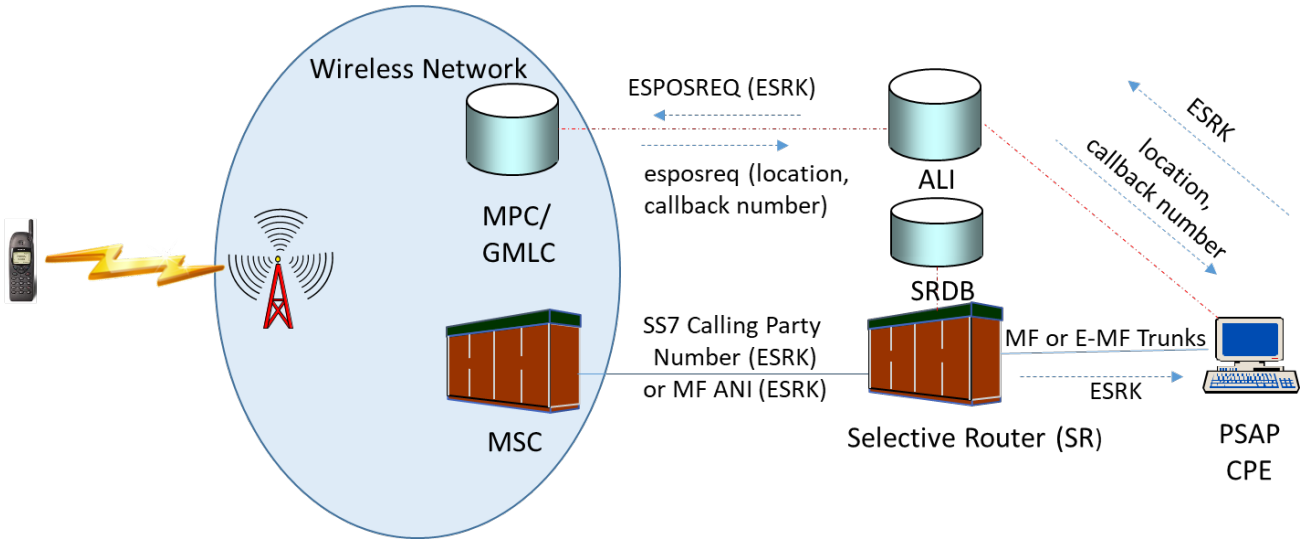



**Figure 5.3: Wireless E9-1-1 – Wireline Compatibility Mode**

## 5.2 i2/Pre-i2 Architectures

The architecture used to support 9-1-1 call delivery in an "i2" or "pre-i2" environment is based on the architectures used for wireless E9-1-1. While there are variations in how i2/pre-i2 architectures are implemented, in a typical i2/pre-i2 environment, 9-1-1 calls originate in a VoIP network and are delivered over MF or SS7 trunks to an SR via an Emergency Services Gateway (ESGW). Instead of delivering an ESRK with the 9-1-1 origination, the VoIP network delivers an Emergency Services Query Key (ESQK) with the call. The SR uses the ESQK to query an SRDB to determine how to route the call and includes the ESQK in the MF signaling sent to the target PSAP. As with wireless WCM, the PSAP uses the ESQK to query the ALI system. In the context of this architecture, the ALI system interacts with a VoIP Positioning Center (VPC) using an E2-like interface, similar to the way it would interact with an MPC/GMLC in a wireless originating network. Upon receiving location and callback information from the VPC, the ALI system passes the information to the PSAP. Figure 5-4 illustrates a typical "i2"/"pre-i2" architecture.

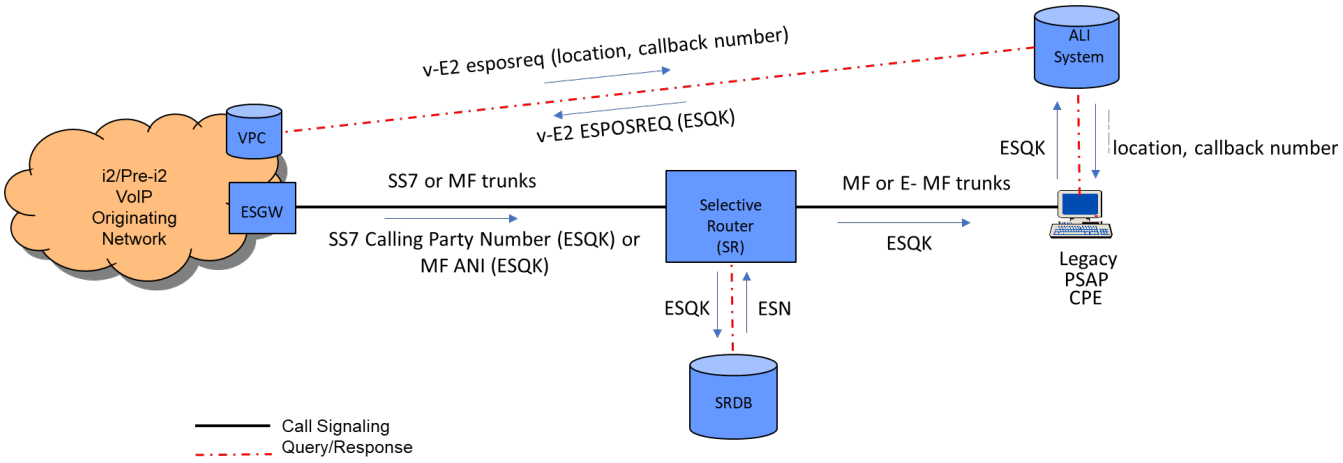



**Figure 5.4: i2/Pre-i2 VoIP 9-1-1 Architecture**

## *5.3 Transitional NG9-1-1 Architecture*

During the transition to end-state NG9-1-1, NG9-1-1 Emergency Services Networks will be required to support emergency calls that originate in legacy (circuit-switched) wireline and wireless networks and must be able to support the delivery of emergency calls to legacy PSAPs that they serve. As a result, gateway functionality will be a required part of transitional NG9-1-1 architectures.

### 5.3.1 Transitional Architectures that Include Legacy Network Gateways

To support emergency calls that originate in legacy networks, the NENA i3 architecture, as specified in NENA-STA-010.3 [Ref 14], and the ATIS IP Multimedia Subsystem (IMS)-based NG9-1-1 Service Architecture, as specified in ATIS-0500032 [Ref 15], include the Legacy Network Gateway (LNG) functional element. The LNG logically resides between the originating network and the NG9-1-1 Emergency Services Network and allows PSAPs served by the NG9-1-1 Emergency Services Network to receive emergency calls from legacy originating networks. The LNG interworks the SS7 or MF signaling received from a legacy originating network to the SIP signaling used in the NG9-1-1 Emergency Services Network. In addition, the LNG is responsible for routing emergency calls to the appropriate element in the appropriate NG9-1-1 Emergency Services Network. To support this routing function, the LNG applies NG9-1-1 specific interworking functionality to legacy emergency calls that allows the information provided in the call setup signaling by the wireline switch or MSC (e.g., calling number/ANI, ESRK, ESRD) to be used as input to the retrieval of a routing location (in the form of a street address or geo coordinate location) from an associated location server/database. The LNG uses this location information to query a call routing function to obtain routing information in the form of a Uniform Resource Identifier (URI). The LNG then forwards the emergency call to a routing element in the NG9-1-1 Emergency Services Network, using the URI provided by the call routing function. The LNG includes callback and location information in the outgoing SIP signaling.

The location server/database associated with an LNG must support mappings from a specific calling number/ANI or pANI (e.g., ESRK, ESRD) value to a location that will result in the emergency call being routed to the target PSAP associated with the calling number/ANI/pANI. To support routing functionality within the NG9-1-1 Emergency Services Network, the LNG must be capable of processing dereference requests for routing location generated by routing elements within the NG9-1-1 Emergency Services Network. In addition to identifying the location to be used for emergency call routing, the LNG is also responsible for providing caller location to PSAPs for emergency calls that originate in legacy networks. To support this functionality, the LNG must also be capable of receiving and processing location dereference requests from i3 PSAPs and Legacy PSAP Gateways. The mechanisms used by an LNG to access caller location are comparable to those used by an ALI system to provide caller location to a PSAP in an E9-1-1 environment (i.e., by accessing provisioned data and steering queries to MPC/GMLCs in wireless originating networks, as appropriate).

Figure 5-5 illustrates a transitional NG9-1-1 architecture that includes an LNG.

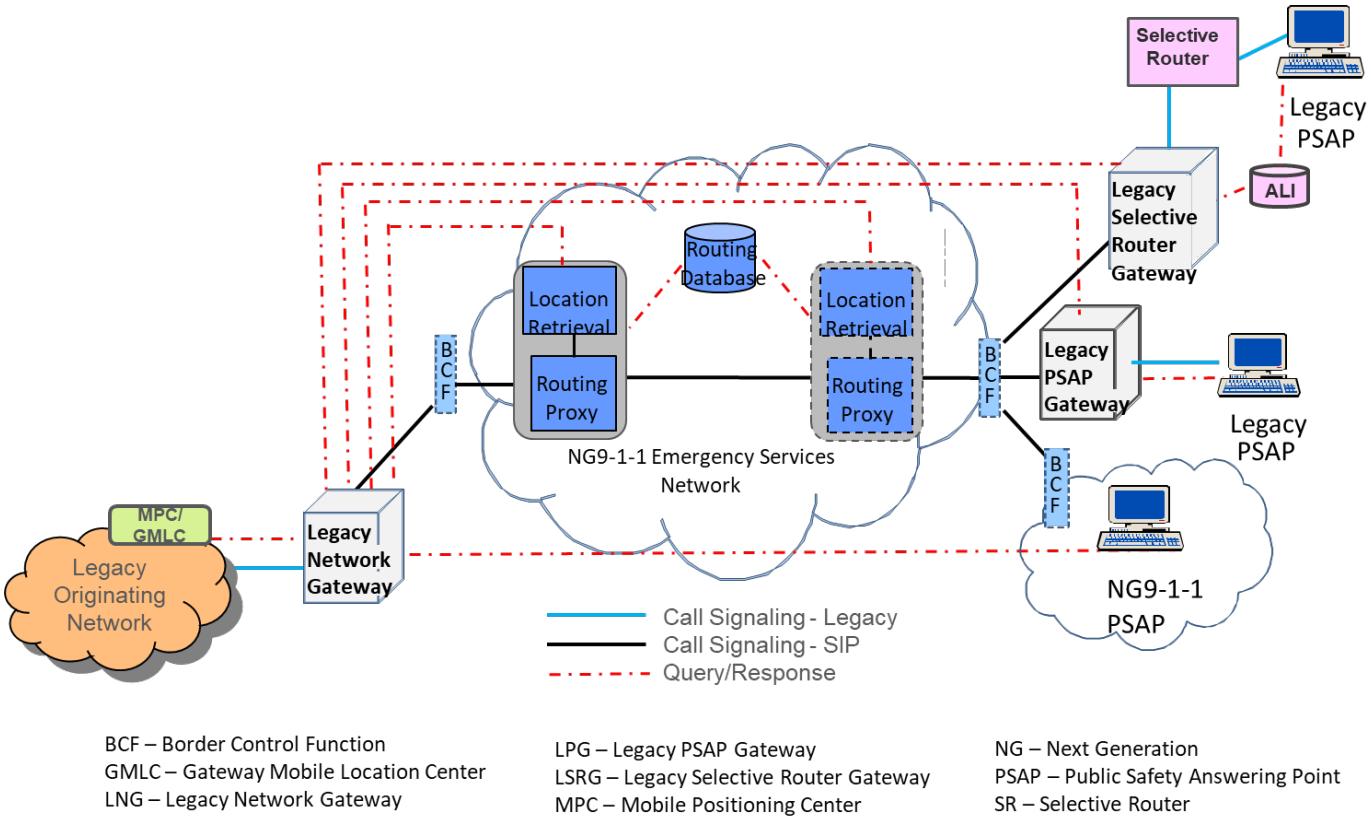



**Figure 5.5: Transitional NG9-1-1 Architecture with LNG**

The LNG in a transitional NG9-1-1 architecture may be operated by the Originating Service Provider (OSP) or by the NG9-1-1 Emergency Services Network Provider. In actual implementations, it is more typical for the NG9-1-1 Emergency Services Network Provider to operate the LNG. Since the LNG is an interworking point in a transitional NG9-1-1 architecture, the entity responsible for operating the LNG is relevant when considering the application of non-IP call authentication solutions to 9-1-1 calls. Specifically, the attestation level associated with a caller identity is based on the relationship between the caller and the entity responsible for authentication of the caller identity. The certificate used to sign the attested caller identity will also depend on where the element that is interacting with the Authentication Service resides. See Clause 6.3 for further discussion.

### 5.3.2 Transitional NG9-1-1 Architectures the Include Legacy PSAP Gateways

A Legacy PSAP Gateway (LPG) is a signaling and media interconnection point between an NG9-1-1 Emergency Services Network and a legacy PSAP. In a transitional NG9-1-1 architecture that includes an LPG, the LPG will receive the same signaling associated with a 9-1-1 call from the NG9-1-1 Emergency Services Network as an i3 PSAP would receive. In addition, the LPG is required to deliver 9-1-1 calls and associated data to legacy PSAPs using the same MF call delivery interfaces and ALI interfaces as the PSAP would use in an E9-1-1 environment. The LPG is expected to provide special processing of the information received in incoming (SIP-based) call setup signaling to facilitate call delivery to legacy PSAPs, to assist legacy PSAPs in obtaining the callback and location information necessary to handle the call and support the dispatch of emergency personnel, and to support feature functionality currently available to legacy PSAPs, such as call transfer.

The LPG will be responsible for interworking SIP signaling received from the NG9-1-1 Emergency Services Network to the Traditional MF or E-MF signaling that is appropriate for the interface over which the call will be delivered to the legacy PSAP. While 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. It is possible that the callback information delivered to an LPG with an emergency call (e.g., associated with a VoIP origination) will not be in the form of (or easily converted to) a 10-digit NANP number. If a legacy PSAP is expecting to receive callback information with the call, and the callback information received by the LPG is not in the form of (or easily converted to) a 10 digit NANP number with an NPA that is appropriate for the target PSAP (i.e., consisting of one of four NPAs supported by a legacy PSAP that supports a Traditional MF interface), the LPG will perform a mapping from the callback information to a locally significant digit string that can be delivered to the legacy PSAP via

Traditional MF or E-MF signaling (as appropriate for the PSAP). The locally significant digit string delivered to the PSAP will be of the form “NPD/NPA-511-XXXX”. The LPG will use the same mechanism to map callback information to a locally significant digit string if the callback information received in call setup signaling is in the form of a 10-digit NANP number, but the NPA is not one that is supported by the PSAP.

If the PSAP expects to receive a location key with the emergency call, the LPG will generate a 10-digit key (pANI) and associate it with the location and other call information that was provided in the incoming signaling from the NG9-1-1 Emergency Services Network. This LPG will pass the pANI to the PSAP via the Traditional MF or E-MF interface (as appropriate for the PSAP) and the PSAP will use it to query the ALI system. If the PSAP expects to receive both callback and location information with the emergency call (i.e., via an E-MF interface) and a pANI of the form NPD/NPA-511-XXXX is sent in the MF sequence corresponding to the callback number, the same digit string can be generated by the LPG and delivered to the legacy PSAP to represent the location information.

Location information received by the LPG will be provided to the legacy PSAP outside of the call setup process via a legacy ALI interface. The LPG will look to the legacy PSAP like an ALI system and the legacy PSAP will query the LPG using the same interface as it would use to query an ALI database. Like an ALI system, when an LPG is queried with an ALI location key (i.e., callback number and/or pANI), the LPG will respond with the location and other non-location information, as appropriate for the query protocol used by the legacy PSAP.

Figure 5-6 illustrates a transitional NG9-1-1 architecture that includes an LPG.

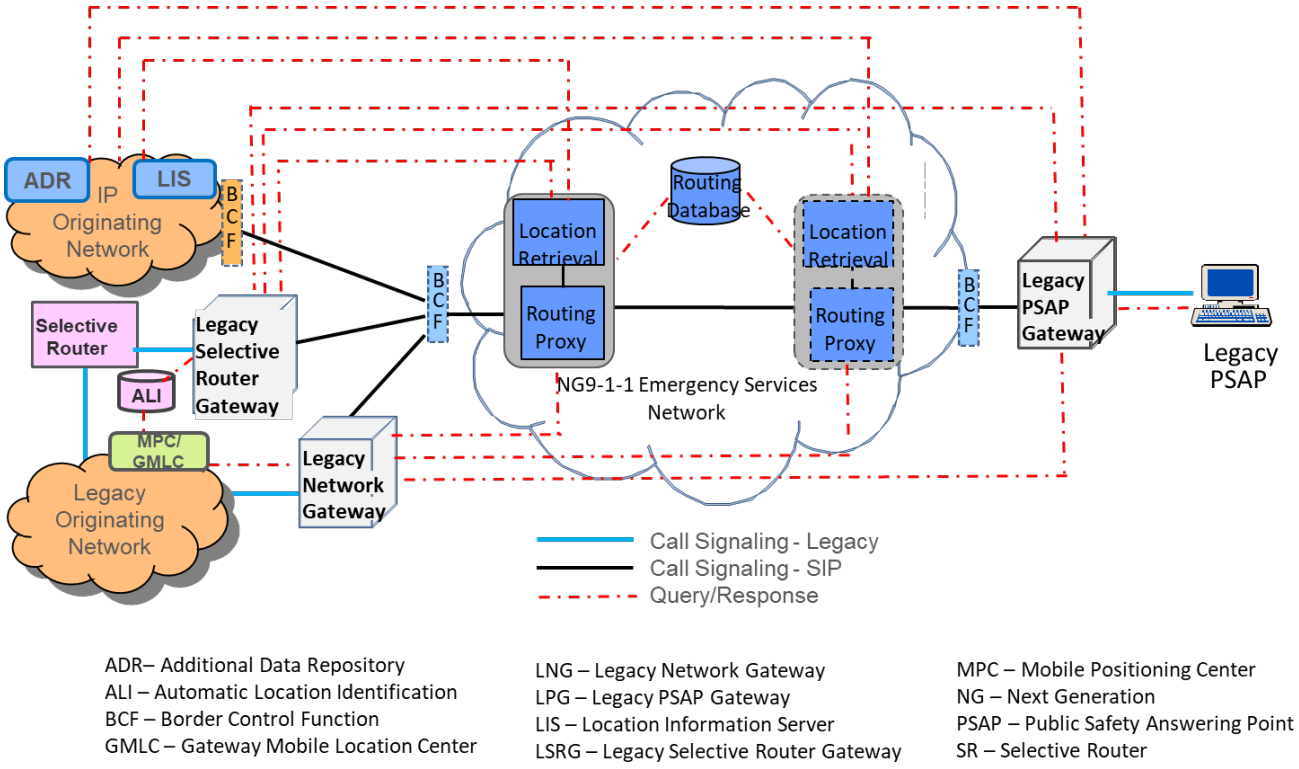



**Figure 5.6: Transitional NG9-1-1 Architecture with LPG**

### 5.3.3 Transitional NG9-1-1 Architectures that Include Legacy Selective Router Gateways

A Legacy Selective Router Gateway (LSRG) is a signaling and media connection point between a legacy SR and an NG9-1-1 Emergency Services Network. The purpose of the LSRG is to allow PSAPs and origination networks of all types (e.g., wireline, wireless, VoIP pre-i2) to migrate from legacy Emergency Services Networks composed of SRs and ALI systems to NG9-1-1 systems, according to different schedules. An ingress LSRG allows emergency originations routed via a legacy SR to terminate on an NG PSAP, as well as allowing calls routed via an NG9-1-1 Emergency Services Network to terminate to a legacy PSAP that is served by an LPG or egress LSRG. An egress LSRG allows emergency calls that are routed via an NG9-1-1 Emergency Services Network to be delivered to a legacy PSAP that is connected to a legacy SR. LSRGs also facilitate transfers of calls between PSAPs that are

served by legacy SRs and PSAPs that are served by NG9-1-1 Emergency Services Networks, regardless of the type of network from which the initial emergency call originated. Clause 5.3.3.1 describes a transitional NG9-1-1 architecture that includes an ingress LSRG. Clause 5.3.3.2 describes a transitional NG9-1-1 architecture that includes an egress LSRG.

### 5.3.3.1 Ingress LSRG Architecture

An LSRG on the ingress side of an NG9-1-1 Emergency Services Network supports an SS7 interface toward the SR, and a SIP interface toward the NG9-1-1 Emergency Services Network. To the SR, the LSRG looks like another SR, interconnected via an SS7 tandem-to-tandem trunk group. The LSRG must support functionality to interwork the SS7 signaling that it receives from the SR with the SIP signaling used in the NG9-1-1 Emergency Services Network. An ingress LSRG is also responsible for routing emergency calls that originate in a network that is connected to the SR to the appropriate (routing) element in the NG9-1-1 Emergency Services Network. To support this routing, the LSRG must apply service-specific interworking functionality to legacy emergency calls to allow the information provided by the originating network (e.g., calling number/ANI, ESRK, ESRD) in the call setup signaling, and passed to the LSRG through the SR, to be used as input to the retrieval of routing and caller location.

The LSRG obtains caller location information by querying a legacy ALI system using the “key” (i.e., calling number/ANI, ESRK, ESRD) provided in call setup signaling. To the ALI system, the LSRG looks like a PSAP. The LSRG obtains routing location either from the ALI system (e.g., for wireline originations) or by mapping the received ESRK/ESRD to a location that will result in the call being routed to the target PSAP. The LSRG uses the routing location to query a call routing function to obtain routing information in the form of a URI. The LSRG must then forward the emergency call/session request to the appropriate element in the NG9-1-1 Emergency Services Network, based on the URI provided by the routing function. The LSRG includes callback and location information in the outgoing SIP signaling sent to the NG9-1-1 Emergency Services Network. The location information populated by the LSRG in outgoing signaling may be “by value” (which is typical for wireline originations) or “by reference” (which is typical for originations from mobile devices).

Since an LSRG may be responsible for generating a location-by-reference, it must support location dereference requests for routing location generated by routing elements within the NG9-1-1 Emergency Services Network, and location dereference requests from i3 PSAPs, LPGs and egress LSRGs for caller location. When an ingress LSRG receives a dereference request for caller location information, it will query the ALI system, and the ALI system will typically steer the query to an MPC/GMLC in a wireless originating network.

Figure 5-7 illustrates a transitional NG9-1-1 architecture that includes an ingress LSRG.

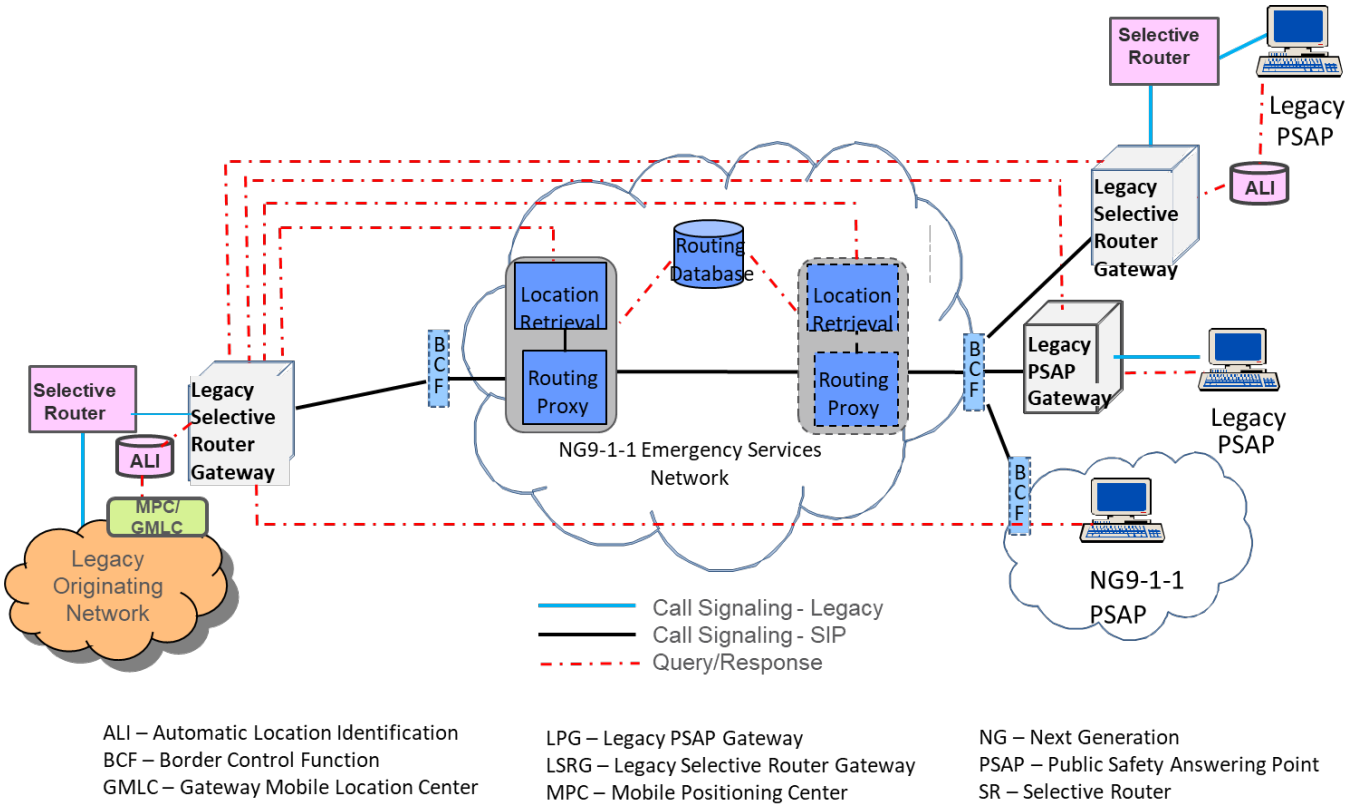



**Figure 5.7: Transitional NG9-1-1 Architecture with Ingress LSRG**

### 5.3.3.2 Egress LSRG Architecture

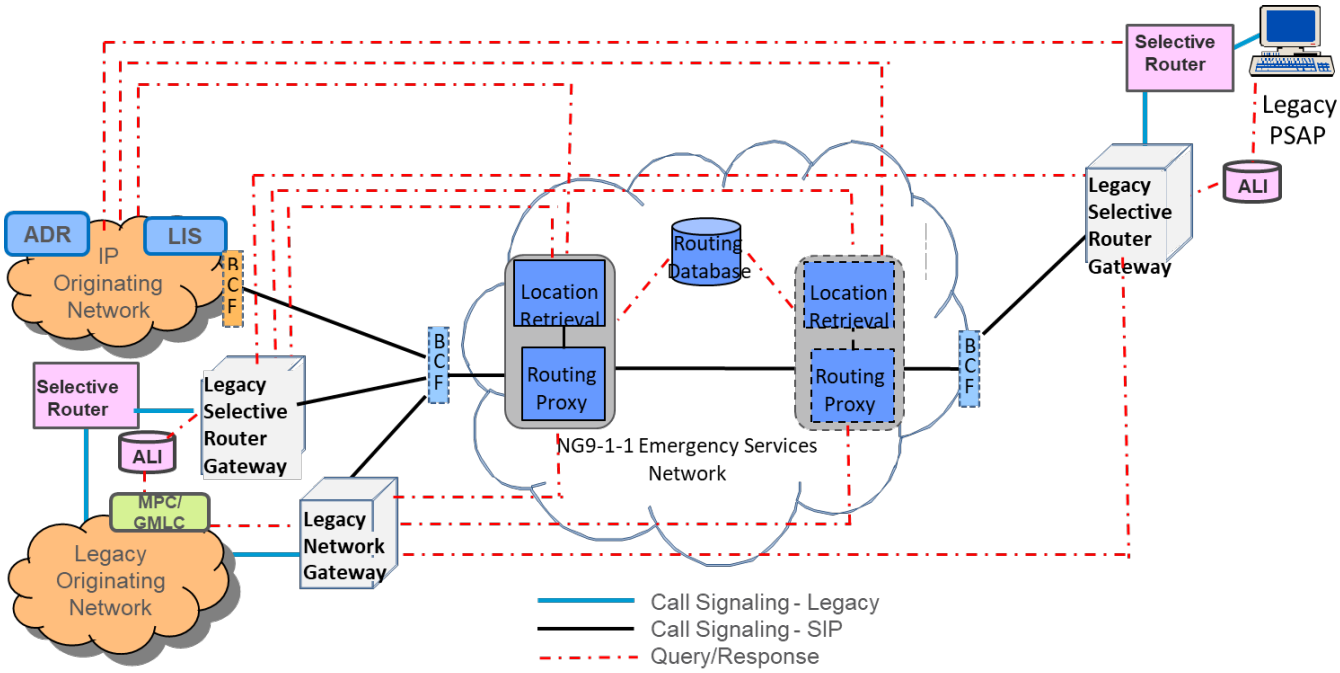
An emergency call that is routed via an NG9-1-1 Emergency Services Network and is destined for a legacy PSAP that is connected to an SR will traverse an LSRG on the egress side of the NG9-1-1 Emergency Services Network. Upon receiving an emergency session request from an NG9-1-1 Emergency Services Network, the LSRG will analyze the signaled information and apply NG9-1-1-specific processing to identify the outgoing trunk group over which the call will be delivered to the interconnected legacy SR, and to ensure that the information delivered to the legacy SR is in an acceptable format.

The LSRG delivers the emergency call to the SR over an SS7-supported tandem-to-tandem trunk group. SS7 tandem-to-tandem interfaces between legacy SRs assume that information such as the PSAP Directory Number, the callback number and/or location keys (i.e., pANIs) signaled to the legacy SR will be in the form of a 10-digit NANP number. It is possible that some emergency originations (e.g., from VoIP callers) will contain callback information that is not in the form of (or easily converted to) a 10-digit NANP number. If callback information is to be delivered to the SR (i.e., in the SS7 Calling Party Number parameter) and it is not in the form of (or easily converted to) a 10-digit NANP number, the LSRG will perform a mapping from the non-NANP callback information to a pseudo callback number that is appropriate for the destination PSAP.

The LSRG will also need to be able to pass a key to the location information associated with the emergency call to the SR, either by itself (i.e., populated in the SS7 Calling Party Number parameter) or in addition to the callback information (where the callback information is populated in the SS7 Calling Party Number parameter and the location key is populated in the SS7 Generic Digits Parameter). An egress LSRG must therefore also generate a 10-digit pANI to associate with the location information received in incoming signaling from the NG9-1-1 Emergency Services Network. (The same digit string can be used to represent both the callback and location information.)

If the SR receives both a callback number (or pseudo callback number) and a pANI (associated with the location information), it will use per-PSAP provisioning to determine what will be signaled forward to the PSAP. The PSAP will use the information received in incoming signaling to query an ALI system to obtain caller location for the call. The ALI will steer the location query back to the LSRG in the same way as it would steer a location query to an MPC/GMLC in a wireless originating network. To support location delivery to legacy PSAPs that are served by

legacy SRs, the LSRG must support the interface protocol used by the interconnected ALI system to query an MPC/GMLC (e.g., the E2 protocol). The location key used in the query to the LSRG will be the pANI (possibly in combination with the callback number/pseudo callback number) created by the LSRG for the emergency call. If the location information received from the NG9-1-1 Emergency Services Network is in the form of a location-by-value, the LSRG will be responsible for returning that location information, as well as the callback number and other non-location information, in the response to the ALI system. If the location information is in the form of a civic location/street address, the LSRG must ensure that the location returned in the ALI response is in a format that is acceptable to the ALI system/PSAP. If the location information received from the NG9-1-1 Emergency Services Network is in the form of a location-by-reference, the LSRG will first have to dereference the location reference to obtain the location value to be returned in the response to the ALI system. Once again, if the location value is in the form of a civic location/street address, the LSRG will have to ensure that location returned in the ALI response is in an acceptable format. Figure 5-8 illustrates a transitional NG9-1-1 architecture that includes an egress LSRG.




ADR– Additional Data Repository
ALI – Automatic Location Identification
BCF – Border Control Function
GMLC – Gateway Mobile Location Center

LNG – Legacy Network Gateway
LIS – Location Information Server
LSRG – Legacy Selective Router Gateway

MPC – Mobile Positioning Center
NG – Next Generation
PSAP – Public Safety Answering Point
SR – Selective Router

**Figure 5.8: Transitional NG9-1-1 Architecture with Egress LSRG**

### 5.3.4 Interconnection of IMS Originating Networks and Legacy Selective Routers

ATIS-0700015 [Ref 6] defines the functional interconnection of an originating IMS network to Emergency Services Networks, as shown in Figure 5.9. The scope of ATIS-0700015 [Ref 6] is to identify, and adapt as necessary, Third Generation Partnership Project (3GPP) Common IMS emergency procedures for applicability in North America to support emergency communications originating from an IMS subscriber (fixed, nomadic, or mobile) and delivered to an Emergency Services IP network (ESInet) or to a legacy SR.

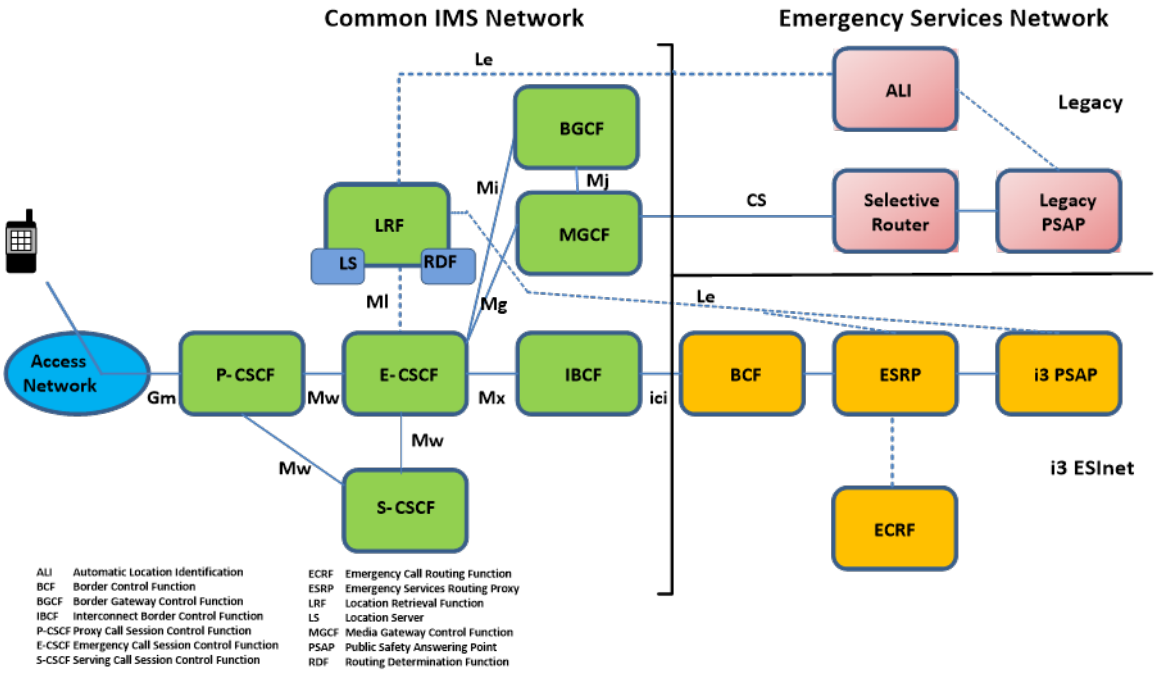



**Figure 5.9: ATIS-0700015 IMS Interconnection Architecture**

This architecture assumes that when an emergency call/session is initiated by User Equipment (UE), it will be sent to a Proxy Call Session Control Function (P-CSCF). The P-CSCF then forwards the emergency call/session request to an Emergency Call Session Control Function (E-CSCF) in the same (originating) network. The E-CSCF forwards the request to the Location Retrieval Function (LRF) to obtain location and/or routing information for that call/session.

UE location information (or an approximation of it) is needed to support the routing mechanism provided by the Routing Determination Function (RDF) element in response to a query from the LRF. If a location value has been provided in the session request from the E-CSCF, the LRF does not have to invoke location retrieval functionality prior to invoking routing determination functionality. If UE location is not available in the session request forwarded by the E-CSCF, the LRF will use a location acquisition technique that is appropriate for the call type to obtain the needed location information.

Having obtained a routing location for the call, the LRF will interact with the RDF, using the location information and a service identifier (i.e., Uniform Resource Name [URN]) as input to the route determination process. Note that, in the case of wireless originations, the LRF will query the RDF with a routing location (i.e., an “Associated Location” which is a pre-provisioned location that is mapped from the cell information) that will result in the RDF returning routing information that reflects bilateral agreements between PSAPs regarding who should receive particular types of calls from specific geographic areas.

The RDF will return routing information (e.g., a Route URI) that will cause the call to be directed either toward an i3 ESInet or toward an SR in a legacy Emergency Services Network. If the call is destined for a legacy Emergency Services Network, the information returned by the LRF to the E-CSCF must be appropriate for the path (i.e., trunk group) over which the call will be delivered by the Media Gateway Control Function (MGCF) to the legacy SR. Calls may be delivered to legacy SRs either with 10 digits of information (i.e., a Reference Identifier **or** a callback number), or with 20 digits of information (i.e., a Reference Identifier **and** a callback number), based on the outgoing trunk group. If the LRF determines that a Reference Identifier is required, it will create one in the form of a 10-digit number and associate it with the call. If a callback number is expected by the SR, the LRF may either include the callback number in its response to the E-CSCF, or the E-CSCF may just use the telephone number that was received in the initial emergency call/session request. Thus, the LRF will always return a Route URI to the E-CSCF and it will either return a Reference Identifier, a callback number, both, or neither (for the case where no Reference Identifier is required and the E-CSCF is expected to use the telephone number received with the emergency call/session request). The E-CSCF will forward the call (via a Breakout Gateway Control Function [BGCF]) to an MGCF for delivery to a legacy SR. The MGCF will be responsible for interworking the incoming SIP signaling to SS7 or MF

signaling, as appropriate for the outgoing trunk group to the legacy SR. The SR uses the Reference Identifier to determine the PSAP (by querying an SRDB) and delivers the call with the Reference Identifier and/or callback number to the legacy PSAP over a Traditional or E-MF interface (as appropriate for the target PSAP).

When a legacy PSAP receives an emergency call that originates in an IMS network and has been routed via a legacy SR, it will use a 10-digit key received in incoming signaling from the SR to query the ALI database for location information. Upon receiving the 10-digit key from the PSAP, the ALI system will consult "steering" data to determine whether the LRF must be queried to obtain location information.

If the key is not present in the steering data, the ALI will retrieve static location (and non-location, e.g., callback) information from its internal database, and return it to the PSAP. If the 10-digit key is contained in the steering data, the ALI will generate an E2 or MLP[12] query to the system identified in the steering data (i.e., the LRF) to obtain location and callback information for the emergency call.

# 6 Application of Alternative Non-IP Caller Authentication Solutions to Legacy and Transitional 9-1-1 Architectures

This clause analyzes the applicability of the alternative approaches to supporting call authentication in a non-IP environment to 9-1-1 calls processed using the legacy E9-1-1 and transitional NG9-1-1 network architectures described in Clause 5.

## *6.1 Call Authentication in an E9-1-1 Environment*

The end-to-end TDM call scenario illustrated in Figure 4.1 most closely addresses how the SHAKEN OOB PASSporT Transmission Involving TDM Networks call authentication mechanism might be applied to a legacy E9-1-1 architecture. It is important to note that the SHAKEN OOB mechanism described in Clause 4.1 assumes that all TDM networks support SS7, so this non-IP call authentication solution would not apply to E9-1-1 architectures that currently use MF signaling to legacy SRs. In addition, the SHAKEN OOB call authentication mechanism requires additional functional elements and interfaces to be accessible to switches in the originating network and the Emergency Services Network. For example, the application of the SHAKEN OOB call authentication mechanism to 9-1-1 calls in an E9-1-1 environment would require that end offices/MSCs route calls to an interworking function rather than to an SR (via a dedicated trunk group). The interworking function would be responsible for interacting with an STI-AS to obtain a "shaken" PASSporT for the call, and with an STI-OOBS to have that PASSporT published to an STI-CPS. Based on flow described in Clause 4.1, the SHAKEN OOB solution assumes that an ISUP REL message with Cause Code 34 will be used to trigger the routing of the 9-1-1 call from the STI-IWF to the SR. The SHAKEN OOB solution also assumes that there is an interworking function in the legacy Emergency Services Network. This interworking function (i.e., the STI-IWF) would be responsible for retrieving the "shaken" PASSporT (via the STI-OOBS) and interacting with the STI-VS to verify it. While ATIS-1000096 [Ref 2] leaves the call handling in a TDM terminating network up to implementation, there would be impacts on existing SR call processing and interfaces to support interactions between an SR and an STI-IWF and the handling of verification status information by the SR (assuming the implementation supports a way of returning the verification results to the SR).

There are also unique challenges associated with defining a mechanism to convey attestation and verification status information to legacy PSAPs with 9-1-1 calls. For legacy PSAPs, the ability to convey attestation or verification status information is significantly limited by the use of legacy MF interfaces for call delivery and legacy ALI interfaces for the delivery of location and some non-location information. For legacy PSAPs that support E-MF interfaces, it might be possible to use spare "II" values to convey attestation and verification information associated with the caller identity, but this would require modifications to the call processing supported by the SR to correctly populate the "II" value in the outgoing E-MF signaling based on attestation and verification status information received from the STI-IWF. There would also be impacts on PSAP Operating Procedures to support the interpretation of the new "II" values by PSAP call takers. For legacy PSAPs that support Traditional MF interfaces, there does not seem to be an MF signaling-based option for conveying attestation and verification status information with a 9-1-1 call due to the significant signaling limitations associated with such interfaces

[12] Note that use of the PSAP to ALI Message (PAM) protocol between the ALI system and the LRF is not supported by the interconnection architecture described in ATIS-0700015 [Ref 6].

While the above procedures could be considered as a possible approach to authenticating caller identity information for wireline 9-1-1 or wireless NCAS originations, where callback information is included in call setup signaling, it is not clear what relevance, if any, these procedures have when a wireless WCM 9-1-1 call is originated. As described in Clause 5.1, the SS7 Calling Party Number parameter in an IAM associated with a WCM call will be populated with an ESRK, not the callback number. The callback number is provided to the PSAP via the ALI system using a separate data interface. While there may still be value in authenticating the ESRK to ensure that it is one that was actually populated by the legacy wireless originating network, and not one that was spoofed by a bad actor, authenticating and verifying the ESRK does not communicate anything about the legitimacy of the callback information.

Consideration should also be given to applying the Extending STIR/SHAKEN Over TDM call authentication mechanism to 9-1-1 calls in an E9-1-1 environment. As described in Clause 4.2, this call authentication approach proposes the use of specific values in SS7 signaling parameters, such as the Screening Indicator in the Calling Party Number parameter, or specific trunk groups, to convey attestation and/or verification status information over TDM interconnections. The mappings between Screening Indicator values (or trunk groups) and attestation levels described in ATIS-1000095 [Ref 4] assume that at least one network involved in processing the call is SHAKEN-capable, and that interworking between SS7 and SIP will need to be performed at some point in the call path. In an E9-1-1 environment, neither the originating network nor the Emergency Services Network is SHAKEN/SIP-capable, so the Extending STIR/SHAKEN Over TDM mechanism may not directly apply. However, the mappings defined between Screening Indicator values (for legacy originating networks that interconnect to SRs using SS7 trunks) and attestation levels could be used as a basis for determining the attestation level and verification status associated with the information signaled in the SS7 Calling Party Number parameter. Based on standards related to E9-1-1 (i.e., ATIS-1000628 [Ref 7]), an SS7 Calling Party Number parameter will be populated with a network-provided number (i.e., Screening Indicator set to “network provided”), unless the call originates from an ISDN interface, the originating switch allows user-provided numbers from ISDN interfaces to be used as calling party numbers, and the user-provided number passes screening. In the latter case, the Screening Indicator associated with the Calling Party Number will have the value “user provided, screening passed”. Based on ATIS-1000628 [Ref 7], a user-provided number that fails screening shall not be sent toward the SR; instead, the main (i.e., network-provided) number shall be sent toward the SR as the calling party number. According to ATIS-1000095 [Ref 4], both a Screening Indicator value of “network provided” and a Screening Indicator value of “user provided, screening passed” would be associated with an attestation level of “A” and a verstat value of “TN-Validation-Passed”.

Since, based on ATIS-1000095 [Ref 4], all allowable Screening Indicator parameter values associated with 9-1-1 originations from legacy originating networks will map to an attestation level of “A” and a verstat value of “TN-Passed-Validation”, it may be sufficient just to know that the call originated in a legacy wireline or wireless network to associate an “A” attestation and a verification status of “TN-Passed-Validation” with the information signaled as the calling number. The type of network that the call originated from is known by the SR based on the incoming trunk group but cannot be determined by the legacy PSAP based on MF signaling associated with a 9-1-1 call. In addition, while the determination of attestation level and verification status using the Extend STIR/SHAKEN Over TDM call authentication approach does not require the implementation of additional SHAKEN-related elements and interfaces in legacy networks, the same issue related to conveyance of attestation and verification status information to legacy PSAPs via the call setup interface applies as for the SHAKEN OOB call authentication mechanism.

The call authentication mechanism described in Clause 4.3, where a “shaken” PASSporT is encoded in the UUI parameter of an SS7 IAM, does not apply in a legacy E9-1-1 environment because standards and existing implementations do not support the delivery of the UUI parameter in an SS7 IAM associated with a 9-1-1 call. Also, this particular call authentication mechanism assumes that, at some point in the call flow, there will be interworking between SIP and TDM/ISUP, and that is not the case in an E9-1-1 environment. In addition, if an SR were able to receive a UUI parameter containing a “shaken” PASSporT, it is not clear what it would do with it, or how it could be used to convey attestation level and verification status information to a legacy PSAP over an MF interface.

Applying any of the non-IP call authentication solutions described in Clause 4 to an E9-1-1 Service architecture would have an impact on the signaling and call processing supported by legacy SRs. Since suppliers of SR equipment are no longer implementing enhancements to those systems, call authentication solutions that require support for new call processing or modifications to signaling interfaces at an SR cannot be viewed as technically feasible. In addition, even if an SR could obtain attestation level and verification status information associated with a 9-1-1 call, based information received via existing SS7 interfaces (or the incoming trunk group), the ability to deliver this information to legacy PSAPs is limited by the MF call delivery interfaces typically supported by legacy PSAPs today.

An alternative approach for supporting caller authentication in an E9-1-1 environment is to use the ALI interface to deliver information that will allow a legacy PSAP to determine the caller identity attestation level and verification status for the call. As described above, in a legacy E9-1-1 environment, caller identity (i.e., callback) information is either "network-provided", or in the case of certain ISDN user interfaces, "user provided, screening passed". In both cases the caller identity information is considered to have a level of trustworthiness that corresponds to an attestation level of "A" and a verification status of "TN-Validation-Passed". Legacy PSAPs that are operating in an E9-1-1 environment can treat the callback number associated with a 9-1-1 call that originates in legacy wireline or wireless networks as if it has an attestation level of "A" and a verification status of "TN-Validation-Passed". A legacy PSAP can identify 9-1-1 calls that originate in legacy wireline or wireless networks based on the Class of Service (COS) delivered via the ALI interface (e.g., a COS value of "Residential" or one of the "Wireless" values). Specifically, COS values associated with legacy wireline and wireless emergency calls can be used by legacy PSAPs to implicitly associate an attestation level of "A" and verification status of "TN-Validation-Passed" with the callback numbers related to such calls. Adding new values to the COS field to support explicit conveyance of attestation level and verification status has been discouraged by Public Safety because of the limited size of the field and the existing complexities associated with interpreting this field by legacy PSAPs. However, using existing COS values received via the ALI interface to implicitly convey attestation level and verification status can provide legacy PSAPs operating in an E9-1-1 environment with a technically feasible way to assess the legitimacy of callback information received with a 9-1-1 call.

## *6.2 Call Authentication in an i2/Pre-i2 Environment*

As described in Clause 5.2, callback information associated with 9-1-1 calls that originate in i2/pre-i2 VoIP networks is typically network-provided and delivered to a legacy PSAP via the ALI interface (after the ALI system interacts with a VPC). In considering the application of the SHAKEN OOB mechanism described in ATIS-1000096 [Ref 2] to an i2/pre-i2 architecture, it might be possible to enhance the ESGW (or another element, like a call server, in the VoIP i2/pre-i2 network) to support interactions with an STI-AS to obtain a "shaken" PASSporT and an interaction with an STI-OOBS to publish that PASSporT to an STI-CPS. However, since the caller identity signaled with the 9-1-1 call will typically contain an ESQK and not the callback number, and there will be no downstream element to retrieve or use the PASSporT information, there is no obvious benefit to making those enhancements. The same considerations limit any benefit associated with applying the Extending STIR/SHAKEN Over TDM approach described in ATIS-1000095 [Ref 4] to 9-1-1 calls that originate in i2/pre-i2 VoIP networks, since the Screening Indicator would not be associated with the callback number and could not be interpreted by the SR to convey caller identity attestation information or verification status. Also, as in the case of 9-1-1 calls from legacy networks, applying the call authentication mechanism described in Clause 4.3 would not be technically feasible for an i2/pre-i2 architecture, since the UUI parameter is not expected to be included in SS7 signaling sent to an SR by an ESGW.

Because the same MF interfaces are used by the SR to deliver 9-1-1 calls to legacy PSAPs in the context of an i2/pre-i2 architecture as are used for 9-1-1 calls originating in legacy networks, the same limitations apply with regard to delivering attestation level and verification status information to legacy PSAPs in call setup signaling. Consideration should again be given to using the ALI interface to deliver attestation level and verification status information to legacy PSAPs. Unlike 9-1-1 calls originating in legacy networks, there is not a specific COS value that is consistently delivered to legacy PSAPs for 9-1-1 calls that originate in i2/pre-i2 VoIP networks. That means that the legacy PSAP cannot determine, based on the COS, that the callback information provided with the call is network-provided. The ability to successfully retrieve a callback number based on interactions between an ALI system and a VPC will allow a PSAP to apply appropriate call handling (as specified in Standard Operating Procedures) based on the knowledge that the callback number is network-provided, even though it has not received an explicit indication of the specific attestation level and verification status.

It is also possible that attestation level and verification status information could be passed explicitly from a VPC to a legacy ALI system and from a legacy ALI system to a legacy PSAP by using the Customer Name field in the Location Description parameters in the v-E2 and legacy ALI interfaces. An i2/pre-i2 VoIP Service Provider that has performed SHAKEN authentication on the caller identity provided with a 9-1-1 call could pass the resulting attestation level and verification status information from the VPC to a legacy ALI system, and from a legacy ALI system to a legacy PSAP, using the Customer Name field in the Location Description parameters in the v-E2 and legacy ALI interfaces. This assumes that i2/pre-i2 VoIP networks have been enhanced to support STIR/SHAKEN and that they will support the real-time updating of the Customer Name field returned by the VPC to indicate the results of the caller identity authentication process.

If the i2/pre-i2 VoIP network provider has not yet implemented STIR/SHAKEN or does not support the ability to update in real-time the Customer Name information populated in the VPC with the attestation level and verification status associated with the callback number, the PSAP may receive an explicit indication that the attestation level

and verification status associated with the callback information is “unavailable” based on provisioning associated with the Customer Name field provided to it by the VPC via the ALI interface. See Clause 7 for further discussion regarding the use of ALI fields to convey attestation level and verification status information.

## *6.3 Call Authentication in Transitional NG9-1-1 Architectures Involving Legacy Network Gateways*

In a transitional NG9-1-1 architecture that includes an LNG, the presence of the gateway should not have any impact on the way that the legacy originating network processes a 9-1-1 call. The only difference is that the trunk group over which the call is routed is connected to an LNG rather than an SR. In considering the application of the call authentication mechanisms described in Clause 4, it is necessary to consider two scenarios: one where the LNG is operated by the OSP and one where the LNG is operated by the NG9-1-1 Emergency Services Network provider. As described in Clause 5.3.1, it is more typical for the NG9-1-1 Emergency Services Network provider to operate the LNG in actual implementations.

If the OOB SHAKEN call authentication mechanism, as described in Clause 4.1, is applied to an architecture that includes an LNG that is operated by the NG9-1-1 Emergency Services Network provider, the approach would most closely resemble the architecture illustrated in Figure 4.3. The impact on the legacy originating network would be the same as described in Clause 6.1, namely that the 9-1-1 call would be routed from a wireline end office or MSC to an STI-IWF. The STI-IWF would be responsible for interacting with an STI-AS, which would create a “shaken” PASSporT for the call and return it to the STI-IWF. The STI-IWF would forward the SIP INVITE with the PASSporT to the STI-OOBS which would publish it to an STI-CPS. Based on Figure 4.3, the LNG would be responsible for performing all of the expected SS7-SIP interworking and NG9-1-1-specific call processing associated with the 9-1-1 call, but in addition, it would interact with the STI-OOBS (by forwarding it the SIP INVITE message prior to sending the INVITE to the NG9-1-1 Emergency Services Network) to support retrieval of the “shaken” PASSporT from the STI-CPS. Since the SIP INVITE message forwarded to it by the LNG would not contain an Identity header with a PASSporT, the STI-OOBS would need to create a JWT, then pass that along with the calling and called party information to the STI-CPS. Upon receiving the “shaken” PASSporT from the STI-CPS, the STI-OOBS would return the SIP INVITE message to the LNG with the “shaken” PASSporT populated in an Identity header. The LNG would then forward the SIP INVITE with the Identity header to the NG9-1-1 Emergency Services Network, which would be responsible for applying SHAKEN verification procedures to the call.

If the LNG is operated by the OSP, the SHAKEN OOB architecture could be modified so that the LNG would replace the STI-IWF in the originating network. Rather than having the STI-IWF interact with the STI-AS, the LNG could instead interact with the STI-AS (after performing all of the call processing required of an LNG, but before forwarding the SIP INVITE to the NG9-1-1 Emergency Services Network), by forwarding it the SIP INVITE message. The STI-AS would perform normal SHAKEN authentication and create the “shaken” PASSporT. The STI-AS would then populate the “shaken” PASSporT in an Identity header and return it to the LNG in a SIP INVITE message. While the OOB SHAKEN call authentication mechanism, as described in Clause 4.1, assumes that the STI-IWF will forward the SIP INVITE with the “shaken” PASSporT to the STI-OOBS so that the “shaken” PASSporT can be published to the STI-CPS, the LNG could just pass the SIP INVITE with the Identity header to the NG9-1-1 Emergency Services Network, which is SIP/SHAKEN-capable, without having the PASSporT published to the STI-CPS, since functional elements in the NG9-1-1 Emergency Services Network, i3 PSAPs, and any gateway elements on the egress side of the NG9-1-1 Emergency Services Network (i.e., LPG or egress LSRG) would be capable of receiving and processing the PASSporT information provided in the Identity header, and SRs, if present in the call path, would not be capable of retrieving PASSporTs from an STI-CPS.

If the LNG is operated by the NG9-1-1 Emergency Services Network provider, and the Extending STIR/SHAKEN Over TDM call authentication mechanism is applied, then the LNG could be enhanced to map the received Screening Indicator value to an Identity header containing a PASSporT with an attestation level of “A” and include a verstat of “TN-Validation-Passed” in the P-Asserted-Identity header or From header (since all Screening Indicator values associated with legacy 9-1-1 calls will map to these values). Likewise, the LNG could use the trunk group over which it received the 9-1-1 call to determine the attestation level and verstat (which would accommodate calls delivered to the LNG via MF trunk groups). It is expected that any trunk group over which a 9-1-1 call was delivered by a legacy originating network to the LNG would have an attestation level of “A” and a verstat value of “TN-Validation-Passed” associated with it. In addition to populating the attestation level in the Identity header and the verstat value, the LNG would also have to include an STI certificate in the Identity header, signing the PASSporT information. In this case the STI certificate would be associated with the NG9-1-1 Emergency Services Network provider. Since, in this scenario, the LNG is operated by the NG9-1-1 Emergency Services Network provider, routing

the 9-1-1 call from the LNG to an ESRP in an i3 ESInet would be viewed as intranetwork routing, so SHAKEN verification (e.g., by having the ESRP interact with the STI-VS) would not need to be performed.

If the Extending STIR/SHAKEN Over TDM approach was in use and the LNG is operated by the OSP, then the processing at the LNG would be the same as described above, with the LNG mapping the Screening Indicator or incoming trunk group to an "A" attestation and verstat value of "TN-Validation-Passed". As above, the LNG would then create an Identity header with a signed PASSporT and populate the verstat in the P-Asserted-Identity header (or From header, if no P-Asserted-Identity header is to be populated). In this case, the certificate in the PASSporT would be associated with the OSP. However, in this scenario, routing the call from the LNG to an NG9-1-1 Emergency Services Network would be viewed as internetwork routing. As a result, any verstat information populated by the LNG would be stripped out by the Border Control Function (BCF)/Interconnection Border Control Function (IBCF) on the ingress side of the NG9-1-1 Emergency Services Network, and the ESRP/IBCF would be expected to interact with an STI-VS to perform SHAKEN verification.

As indicated in Clause 6.1, the SS7 signaling associated with a 9-1-1 call is not expected to include a UUI parameter. In addition, the non-IP call authentication mechanism that relies on populating a "shaken" PASSporT in a UUI parameter, as described in Clause 4.3, assumes that the 9-1-1 call has originated in a SIP-capable network and encounters TDM interworking along the call path. As a result it is not expected that the PASSporT Encoded in ISUP UUI mechanism would apply to a transitional NG9-1-1 architecture that includes an LNG.

## *6.4 Call Authentication in Transitional NG9-1-1 Architectures Involving Legacy PSAP Gateways*

As described in Clause 5.3.2, a transitional NG9-1-1 architecture that includes an LPG assumes that the LPG will receive the same signaling from an ESRP in an i3 ESInet (or E-CSCF in an IMS NG9-1-1 Emergency Services Network) associated with a 9-1-1 call as an i3 PSAP would receive. The LPG is required to deliver 9-1-1 calls and associated data to legacy PSAPs using the same MF call delivery interfaces and ALI interfaces as the PSAP would use in an E9-1-1 environment. Since a PSAP connected to an LPG supports the same interfaces as in an E9-1-1 environment, the same limitations apply as were described in Clause 6.1 with respect to delivering caller authentication information to the legacy PSAP with the 9-1-1 call. The main difference is that a SHAKEN-capable i3 ESInet will deliver an Identity header and verstat to the LPG (assuming upstream networks also support SHAKEN or some form of non-IP caller authentication). As described in Clause 6.1, it might be possible to convey attestation and verstat information to a legacy PSAP with a 9-1-1 call by using spare "II" values, if the PSAP supports an E-MF interface. Since LPG systems are currently under development, the modifications in call processing at the LPG would be more easily accommodated than for a legacy SR. However, unlike 9-1-1 calls processed in an E9-1-1 environment, where the calling number information signaled with calls from legacy wireline and wireless originating networks will be associated with an "A" level attestation and a verstat value of "TN-Validation-Passed", an LPG will receive 9-1-1 calls that originate in either legacy or NG/VoIP originating networks, and could receive an Identity header that indicates an attestation level of "A", "B", or "C" and a verstat value of "TN-Validation-Passed", "TN-Validation-Failed" or "No-TN-Validation". Many more "II" values would be required to support the conveyance of all of the combinations of attestation level and verstat; particularly if the "II" value continues to be used to convey "flashing" versus steady display to the PSAP CPE. These values would need to be properly interpreted by the PSAP call taker. Also, as described in Clause 6.1, there does not seem to be an MF signaling-based option for conveying attestation and verstat information with a 9-1-1 call to legacy PSAPs that support Traditional MF interfaces due to the significant signaling limitations associated with these types of interfaces.

Clause 6.1 also discusses the use of the ALI interface to convey attestation level and verification status information to a legacy PSAP. Specifically, it describes the use of COS information delivered over the ALI interface to implicitly convey attestation level and verstat information to a legacy PSAP. Since, in an E9-1-1 environment an attestation level of "A" and a verstat value of "TN-Validation-Passed" is the only combination of values that applies for legacy wireline and wireless originations (because the callback number associated with an emergency call will either a network-provided number or a user provided number that has passed screening), using a COS applicable to a wireline or wireless origination would be sufficient to implicitly convey the attestation level and verstat value. However, because LPGs will receive more combinations of attestation level and verification status and will process calls that originate in either legacy or NG/VoIP originating networks, multiple new COS values would need to be assigned and interpreted by the legacy PSAP call taker if COS were used to convey attestation and verification status information. The LPG would need to derive the COS value based on a combination of the attestation level received in the Identity header, the verstat value received in the P-Asserted-Identity or From header, and the Additional Data associated the call (which would convey information regarding the type of service used in originating the 9-1-1 call). As described in Clause 6.1, adding new values to the COS field to support explicit conveyance of

attestation level and verification status has been discouraged by Public Safety because of the limited size of the field and the existing complexities associated with interpreting this field by legacy PSAPs. As described in Clause 6.2, an alternative is to use the “Customer Name” field to convey attestation and verification status information via the ALI interface between the LPG and the legacy PSAP. Another alternative for conveying attestation level and verification status over the ALI interface is the “Comments” field. See Clause 7 for further discussion regarding the use of the Customer Name field or Comments field for conveying attestation and verification status information.

## *6.5 Call Authentication in Transitional NG9-1-1 Architectures Involving Legacy Selective Router Gateways*

As described in Clauses 5.3.3.1 and 5.3.3.2, LSRGs support the interconnection of legacy SRs and NG9-1-1 Emergency Services Networks and may appear on the ingress side of the NG9-1-1 Emergency Services Networks (to support originating networks that are served by SRs) or on the egress side of the NG9-1-1 Emergency Services Network (to support legacy PSAPs that are served by SRs).

### 6.5.1 Call Authentication at an Ingress LSRG

An ingress LSRG has many of the same characteristics as an LNG, except that it receives 9-1-1 calls over SS7 trunk groups from legacy SRs. In considering the application of the SHAKEN OOB call authentication mechanism to 9-1-1 calls that are routed via ingress LSRGs, Figure 4.3 would apply, and the impact on the legacy originating network would be the same as described in Clauses 6.1 and 6.3, namely that the 9-1-1 call would be routed from a wireline end office or MSC to an STI-IWF. The STI-IWF would be responsible for interacting with an STI-AS, which would create a “shaken” PASSporT for the call and return it to the STI-IWF. The STI-IWF would forward the SIP INVITE with the PASSporT to the STI-OOBS which would publish it to an STI-CPS. However, in this case the call would traverse an SR and be delivered to the ingress LSRG over an SS7 trunk group with essentially the same information that the SR received from the end office/MSC, with the following exception: the SS7 Called Party Number would be required to contain the digits “911”[13]. In this scenario, the LSRG would be responsible for performing SS7-SIP interworking and NG9-1-1-specific call processing associated with the 9-1-1 call. In the context of the SHAKEN OOB call authentication mechanism, the LSRG would also interact with the STI OOBS (by forwarding it the SIP INVITE message prior to sending it to the NG9-1-1 Emergency Services Network) to support retrieval of the “shaken” PASSporT from the STI-CPS. Since the SIP INVITE message forwarded to it by the LSRG would not contain an Identity header with a PASSporT, the STI-OOBS would need to create a JWT, then pass that along with the calling and called party information to the STI-CPS. Upon receiving the “shaken” PASSporT from the STI-CPS, the STI-OOBS would return the SIP INVITE message to the ingress LSRG with the “shaken” PASSporT populated in an Identity header. The ingress LSRG would then forward the SIP INVITE with the Identity header to the NG9-1-1 Emergency Services Network, which would be responsible for applying SHAKEN verification procedures to the call.

In considering the application of the Extending STIR/SHAKEN Over TDM call authentication mechanism to a transitional architecture involving an ingress LSRG, the LSRG could be responsible for mapping the received Screening Indicator value to an Identity header containing an attestation level of “A” and populating a verstat value of “TN-Validation-Passed” (since all Screening Indicator values associated with legacy 9-1-1 calls will map to these values) in the P-Asserted-Identity header or From header. In addition to populating the attestation level in the Identity header and the verstat value in the P-Asserted-Identity or From header, the LSRG would also have to include a certificate in the Identity header, signing the PASSporT information. In this case the certificate would be associated with the E9-1-1 System Service Provider (who is assumed to be responsible for operating the ingress LSRG). Any verstat information populated by the LSRG would be stripped out by the BCF/IBCF on the ingress side of the NG9-1-1 Emergency Services Network, and the ESRP/IBCF would be expected to interact with the STI-VS to have SHAKEN verification procedures applied to the PASSporT information in the Identity header.

Considerations related to the use of the call authentication mechanism where a “shaken” PASSporT is encoded in an SS7 UUI parameter are the same as for the LNG scenario described in Clause 6.3. SS7 signaling associated with a 9-1-1 call is not expected to include a UUI parameter and the call authentication mechanism described in Clause 4.3 is intended to apply to SIP originations that transit TDM networks. It is unlikely, therefore, that a call authentication mechanism that relies on populating a “shaken” PASSporT in a UUI parameter would apply to an ingress LSRG in a transitional NG9-1-1 architecture.

[13] The SS7 Called Party Number parameter in an IAM associated with a wireline emergency origination may contain the digits “911”, “11”, “1”, or no digits when an emergency call is delivered to an SR over a dedicated SS7 trunk group.

### 6.5.2 Call Authentication at an Egress LSRG

As described in Clause 5.3.3.2, an egress LSRG takes the SIP signaling received from an NG9-1-1 Emergency Services Network and generates SS7 signaling associated with 9-1-1 calls toward a legacy SR. An egress LSRG must also be capable of processing location queries steered to it by an ALI system (e.g., using the E2 protocol). Like an LPG, an egress LSRG will receive a SIP INVITE from an ESRP in an i3 ESInet (or an E-CSCF in an IMS NG9-1-1 Emergency Services Network) that contains the same information that an i3 PSAP would receive. Assuming that the NG9-1-1 Emergency Services Network and other upstream networks support call authentication, it is expected that the SIP INVITE message delivered to the egress LSRG will include an Identity header containing attestation information, and a P-Asserted-Identity or From header containing a verstat. If the egress LSRG supports the OOB SHAKEN call authentication mechanism then, strictly speaking, it would be responsible for passing the SIP INVITE to an STI-OOBS so that the PASSporT information can be published to an STI-CPS, and the legacy SR would be responsible for also interacting with an STI-OOBS via an STI-IWF to retrieve the PASSporT from the STI-CPS. However, the OOB SHAKEN mechanism does not consider architectures like those involving egress LSRGs, where the verification is performed by an upstream network (i.e., the NG9-1-1 Emergency Services Network) and it is the role of an element in the terminating network (in this case the E9-1-1 Network) to pass the SHAKEN information through a TDM network to the called party over an MF interface. Although the egress LSRG will receive the PASSporT and verstat information via SIP signaling from the NG9-1-1 Emergency Services Network, and is responsible for interworking between SIP and SS7, there is no value in having the egress LSRG publish PASSporT information to an STI-CPS because it will not be possible to enhance SR functionality to support the retrieval of PASSporTs from an STI-CPS, or to enhance the MF call delivery interface to support the delivery of attestation and verification status information to a legacy PSAP.

The Extending STIR/SHAKEN Over TDM call authentication mechanism will allow an egress LSRG to map the attestation level and verstat information received in the SIP INVITE message from the NG9-1-1 Emergency Services Network to an appropriate Screening Indicator value for conveyance to the SR. However, once the call is delivered to the SR, the same issues apply as for the E9-1-1 architecture described in Clause 6.1 with regard to delivering attestation level and verification status information to the legacy PSAP with the call using MF signaling.

Similarly, an egress LSRG could encode the “shaken” PASSporT information received in an Identity header in an SS7 UUI parameter, but even if the SR was capable of receiving and processing that information (which would likely require some updates to the processing at an SR), the same issues would apply regarding the ability to deliver attestation level and verification status information to the legacy PSAP over an MF call delivery interface.

One unique characteristic of the egress LSRG architecture is that it will deliver location and non-location information in response to location requests steered to it by the ALI system, typically using an E2 interface. The Location Description parameter within an E2 response, as defined in NENA-STA-018.2-2021 (originally 05-001) [Ref 8], includes a one character alphanumeric “Class of Service” field, a 32-character “Customer Name” field, and a 30-character “Comments” field. As described in Clause 6.4, the “Customer Name” and “Comments” fields provide a viable means of conveying attestation level and verification status information to legacy PSAPs. See Clause 7 for further discussion.

## *6.6 Conveyance of Caller Authentication Information Between an IMS Originating Network and a Legacy SR*

As indicated in Clause 5.3.4, ATIS-0700015 [Ref 6] describes the interconnection of IMS originating networks with legacy SRs and i3 ESInets. ATIS-0700015.v005 describes the application of SHAKEN caller identity authentication procedures to 9-1-1 calls that are routed to i3 ESInets. This clause considers the possibility of applying call authentication mechanisms to 9-1-1 calls that are routed from an IMS originating network to a legacy SR.

Since the SHAKEN framework defined in ATIS-1000074 [Ref 9] specifies that SHAKEN authentication should be applied after originating call processing (i.e., after routing determination) has been performed, the procedures to apply SHAKEN to 9-1-1 calls destined for an i3 ESInet, as described in ATIS-0700015.v005, use the Ms interface between the IBCF and the STI-AS for creating/signing the “shaken” PASSporT. If the concept of SHAKEN authentication is extended to 9-1-1 calls that are routed to legacy SRs, the functionality performed by the MGCF would need to be enhanced to support authentication of the caller identity information associated with such calls.

The SHAKEN OOB architecture illustrated in Figure 4.2 assumes that an MGCF in a SIP/SHAKEN-capable network that is going to deliver a call over a TDM interface to an interconnected TDM network will interact with an STI-OOBS to publish a “shaken” PASSporT created by a SHAKEN-capable originating network to an STI-CPS. The architecture depicted in Figure 4.2 also assumes that a switch in a terminating TDM network, in this case the SR in an E9-1-1 Emergency Services Network, will interact with an STI-IWF which will interwork the incoming TDM

signaling to a SIP INVITE message and pass the SIP INVITE message to an STI-OOBS. Since there will be no Identity header included in the SIP INVITE received by the STI-OOBS, the STI-OOBS will need to create a JWT and send it along with the calling and called numbers associated with the call, to the STI-CPS. Upon receiving a SIP INVITE message back from the STI-OOBS with an Identity header containing the "shaken" PASSporT, the STI-IWF is expected to invoke SHAKEN verification by passing the SIP INVITE with the Identity header to an STI-VS. As described in Clause 6.1, ATIS-1000096 [Ref 2] leaves to implementation the call processing applied by a TDM terminating network after the verification status (verstat) is received by the STI-IWF. The same challenges exist for this interconnection architecture as for several of the scenarios described above with regard to the impacts on legacy SRs and the conveyance of attestation and verstat information to legacy PSAPs over MF call delivery and legacy ALI interfaces. Applying SHAKEN OOB call authentication procedures to this call scenario will place new requirements on legacy SRs to support additional functionality and interfaces for PASSporT retrieval, as well as to process the attestation and verstat information returned and to convey the information to a legacy PSAP with a 9-1-1 call.

In considering the application of the Extending STIR/SHAKEN Over TDM call authentication mechanism to a transitional architecture that interconnects an IMS originating network and a legacy SR, the MGCF could be responsible for interacting with the STI-AS to sign the caller identity information and would be responsible for mapping the received attestation level and verstat values to the appropriate Screening Indicator, assuming the interface to the SR is an SS7 interface. If the interface to the SR is an MF interface, the MGCF could choose an outgoing trunk group that is appropriate for the attestation level/verstat value. If the P-CSCF in the IMS originating network is responsible for performing attestation of the calling number associated with a 9-1-1 call (which depends on local policy) and inserting a verstat value in the P-Asserted-Identity for From header, then the MGCF will have sufficient information to generate the outgoing SS7 Screening Indicator (or to pick the appropriate outgoing trunk group) without actually interacting with the STI-AS. Assuming that the same or a comparable reference point to the one used by an IBCF to access the STI-AS is used by an MGCF to access the STI-AS, the STI-AS will only be responsible for signing the "shaken" PASSporT associated with the call. Alternatively, the MGCF could forward the SIP INVITE message to the STI-AS for authentication and signing prior to forwarding the call the legacy SR. Either of these approaches would require further standards development work in 3GPP. In addition, enhancements to SR processing would be needed to interpret the Screening Indicator values signaled by the MGCF and the same limitations with regard to delivering attestation level and verification status information to legacy PSAPs via MF call delivery interfaces would apply as in several of the previously described transitional architectures.

To support the application of the call authentication mechanism that encodes an STI PASSporT in an SS7 UUI parameter to this IMS interconnection architecture, the MGCF could interact with the STI-AS to obtain a PASSporT containing signed caller identity information for the call, then encode that PASSporT in a UUI parameter within the SS7 IAM it sends to the SR. However, as described above, new standards related to the MGCF would need to be developed to support interactions between an MGCF and an STI-AS, as well as to support the encoding of the PASSporT information in the UUI parameter. In addition, enhancements to legacy processing and interfaces would be needed to allow the SR to receive and process the UUI and convey the attestation level information to a legacy PSAP via an MF interface.

Since, in this interconnection scenario, the call is being routed to a TDM terminating network (i.e., a legacy Emergency Services Network) that does not currently support STI-VS functionality (or access to it), there may not be value in having the IMS originating network go through the process of creating and signing a "shaken" PASSporT, since a "shaken" PASSporT will not be used by any downstream elements. Regardless of the mechanism used to convey attestation level and verstat information to the legacy SR, the same issues will apply with regard to having the SR process this information and deliver it to a legacy PSAP with the 9-1-1 call.

Like the egress LSRG architecture described in Clauses 5.3.3.2 and 6.5.2, an E2 interface will be used by a legacy ALI system to query an LRF for location and non-location information associated with a 9-1-1 call in the context of the interconnection architecture described in ATIS-0700015 [Ref 6]. If the IMS originating network supports population of attestation and verstat information by the P-CSCF, the LRF will receive this information in the SIP INVITE message sent to it by an E-CSCF. It is therefore possible that the LRF could use one of the E2 fields described in Clause 7 (i.e., "Customer Name" or "Comments") to convey attestation level and verstat information to an ALI system, which would then pass the information over an ALI interface to a legacy PSAP. However, population of the attestation level in the SIP Attestation-Info parameter and a verstat parameter in a P-Asserted-Identity header in an INVITE message associated with a 9-1-1 call is not currently required of a P-CSCF operating in an IMS originating network; population of this information by a P-CSCF is currently left to local policy. If the P-CSCF does not support population of the attestation level and verstat, the LRF will not be able to convey this information to the ALI system in an E2 response so that the ALI system can deliver it to the legacy PSAP. Further study will be needed

to identify an alternate mechanism for delivering attestation level and verification status information to legacy PSAPs using the interconnection architecture described in ATIS-0700015 [Ref 6], if the P-CSCF in an IMS originating network does not support population of this information in the appropriate fields within a SIP INVITE message associated with a 9-1-1 call.

# 7 Conveyance of Call Authentication Information Via the ALI Interface

Due to the limitations in the MF call delivery interfaces, and the infeasibility of updating the call processing or interfaces supported by legacy SRs, this clause examines the use of the ALI interface to support the conveyance of attestation level and verification status information to legacy PSAPs in E9-1-1 and transitional NG9-1-1 architectures. Specifically, this clause considers the use of the COS, Customer Name, and Comments fields to convey attestation level and verification status information.

As described in Clause 6.1, in the context of an E9-1-1 architecture, COS may be used to *implicitly* convey an attestation level of "A" and verification status of "TN-Validation-Passed" because the callback numbers associated with legacy wireline or wireless emergency originations are provided or verified by the OSP, and network-provided caller identity is viewed as being the most trustworthy. However, as described in Clause 6.2, due to variability of COS values used in the context of i2/pre-i2 architectures, the COS cannot be used to unambiguously identify the call as having originated in an i2 VoIP network. In addition, use of COS to convey attestation level and verification status to legacy PSAPs in transitional NG9-1-1 architectures, such as those described in Clause 6.4, would require the definition of multiple new COS values due to the need to convey all potential combinations of attestation level and verification status that could be delivered to an LPG by an NG9-1-1 Emergency Services Network. As noted above, adding new values to the COS field to support explicit conveyance of attestation level and verification status has been discouraged by Public Safety because of the limited size of the field and the existing complexities associated with interpreting this field by legacy PSAPs.

A viable alternative for conveying attestation level and verification status information to legacy PSAPs that are operating in transitional architectures that involve LPGs and LSRGs, and in architectures that support interconnection with IMS originating networks or SHAKEN-capable i2/pre-i2 VoIP networks is the use of the Customer Name field. The Customer Name field is currently defined to be a 32-byte alphanumeric field that is supported by legacy ALI and E2 interfaces. NENA-STA-015.10-2018 (formerly NENA 02-010) [Ref 8] suggests a renaming of the "Customer Name" field to "Customer Name/Service" field to more consistently reflect how the field is currently being used and how it may be used in the future. Clause 19 of NENA-STA-015.10-2018 [Ref 8] describes seven standardized Service Descriptions for the Customer Name/Service field, that may be used alone or in combination with end user customer name or service provider name, to provide guidance to PSAP call takers regarding what location information to give priority to during emergency call handling. Given its size and the precedent set for extending its use beyond just carrying customer name information, the Customer Name field provides a viable alternative for conveying attestation level and verification status information to legacy PSAPs via the ALI interface.

Another ALI data field that may be used to convey attestation level and verification status to legacy PSAPs is the Comments field. The Comments field is a 30-byte alphanumeric field that is used to convey optional notes that may be displayed to the PSAP. One existing use for the Comments field is the conveyance of additional information associated with Multi-Line Telephone Systems (MLTS) users. Like the Customer Name field, the Comments field is supported by both legacy ALI interfaces and E2 interfaces, which makes it a viable alternative for conveying attestation level and verification status information in transitional NG9-1-1 architectures that include LPGs or egress LSRGs. One advantage associated with using the Comments field to convey attestation level and verification status information is its size. Another advantage is its flexibility regarding the type of information that it can convey. The main disadvantage associated with using the Comments field to convey attestation level and verification status information is that it is not universally deployed or consistently used. Consideration must also be given to whether there is sufficient space to display attestation and verification status information in this field to PSAP call takers.

## *7.1 Proposed Formats for Call Authentication Information in ALI Data*

While this document presents two technically viable options for explicitly conveying attestation level and verification status information to legacy PSAPs via the ALI interface, there are many local variations of ALI interface standards that have been deployed. In addition, the amount of space available and the layout of that information on PSAP displays varies based on the type of equipment deployed. While the adoption of a single solution for providing attestation level and verification status information to legacy PSAP call takers is unlikely, this document provides

Public Safety with the tools to convey caller authentication information to legacy PSAPs, should a 9-1-1 Authority or Public Safety agency determine it is desirable to do so. With that objective in mind, this clause describes data formats that can be used to convey attestation level and verification status information to legacy PSAPs via the ALI/E2 interface in the Customer Name or Comments field.

As described in Clause 5.2.4 of ATIS-1000074 [Ref 9], the possible attestation levels associated with caller identity are: “A”, “B” and “C”. In addition, based on input from Public Safety, it would also be desirable to provide an explicit indication to PSAP call takers when attestation level information is unavailable/not provided (e.g., indicated by the value “U”). The possible caller identity verification status (‘verstat’) values, as specified in 3GPP TS 24.229 [Ref 10], are: “TN-Validation-Passed”, “TN-Validation-Failed” and “No-TN-Validation”. These ‘verstat’ values could be represented in the Customer Name/Service or Comments field by the values “P”, “F”, and “N”. Once again, a value of “U” could be used to represent “unavailable”.

While the Customer Name/Service field allows for up to 32 alphanumeric characters, and the Comments field up to 30 alphanumeric characters, it is important to format the attestation level and verification status information as efficiently as possible. This Technical Report recommends the use of the characters “AL” to identify “attestation level” information, and the characters “VS” to identify “verification status” information. Each identifier will be followed by a hyphen and then the appropriate single-letter value. For example, an attestation level of “A” would be conveyed in the Customer Name/Service field or Comments field as “AL-A”, and a verification status of “TN-Validation-Passed” would be conveyed as “VS-P”. Attestation level and verification status information should be appended to any pre-existing information (e.g., name, service) in the ALI field. Note that any characters beyond the 32 allowed for Customer Name/Service field or the 30 allowed for the Comments field will be truncated.

# 8 Conclusion

This Technical Report discusses call authentication in the context of emergency services offered using legacy E9-1-1 and transitional NG9-1-1 architectures. Specifically, this Technical Report assesses the applicability of the non-IP call authentication alternatives specified by the ATIS Non-IP Call Authentication Task Force to legacy E9-1-1 and transitional NG9-1-1 architectures. To support this analysis, Clause 4 of the Report describes the functions and interfaces associated with the alternative non-IP call authentication mechanisms, as they have been defined to support non-emergency calls. Clause 5 of the report then provides a description of various legacy E9-1-1 and transitional NG9-1-1 architectures under which non-IP call authentication must be considered.

The analysis provided in this Technical Report emphasizes the limitations of the elements and interfaces associated with the legacy portions of E9-1-1 and transitional architectures. In particular, the inability to enhance the functionality of legacy SRs or the MF interfaces used to deliver emergency calls to legacy PSAPs significantly reduces the applicability of the non-IP call authentication mechanisms described in Clause 4 to 9-1-1 calls that are destined for legacy PSAPs. As described in Clause 6.3, there may be certain scenarios where a transitional NG9-1-1 architecture that includes an LNG (where the emergency call is subsequently delivered to an i3 PSAP) may be able to work with legacy originating networks that have implemented the SHAKEN OOB or Extending STIR/SHAKEN Over TDM non-IP call authentication mechanisms. Some enhancements to the LNG would be needed to support the functions and interfaces that would allow an LNG to publish or retrieve PASSporT information from an STI-CPS, or to perform the interworking associated with the Extending STIR/SHAKEN Over TDM mechanism.

Where emergency (9-1-1) calls are destined for legacy PSAPs, this Technical Report describes the use of the ALI interface (as well as the E2 interface in the case of transitional NG9-1-1 architectures that include an egress LSRG) to make attestation level and verification status information available to legacy PSAPs either implicitly or explicitly. For E9-1-1 architectures, COS information identifying the type of network (i.e., legacy wireline or wireless) that the call originated from can be used to implicitly associate an attestation level of “A” and verification status of “TN-Validation-Passed” with the callback information provided to the PSAP related to a 9-1-1 call. In the context of an i2/pre-i2 architecture, the Customer Name field provided by a VPC in response to a query from an ALI system can be used to convey attestation level and verification status information. Likewise, the Customer Name/Service or Comments field can be used to deliver attestation level and verification status information to legacy PSAPs via the ALI interface. Clause 7.1 recommends a way of formatting attestation level and verification status information so that it can be consistently conveyed via an ALI interface in a Customer Name/Service or Comments field.

While this Technical Report presents two technically viable options for explicitly conveying attestation level and verification status information to legacy PSAPs via the ALI interface, it is important to recognize that, while ALI interface standards exist (e.g., NENA-STA-015.10-2018 [Ref 8]), implementations reflect many local variations of these standards. In addition, the amount of space available and the configuration used on PSAP CPE to display

call-related information to PSAP call takers varies based the type of equipment deployed. As a result, it is unlikely that there will be a single solution for providing attestation level and verification status information to all legacy PSAP call takers. However, as described in Clause 7.1, this Technical Report provides Public Safety with the tools to convey caller authentication information to legacy PSAPs in a consistent manner, should a 9-1-1 Authority or Public Safety agency determine it is desirable to do so.