ATIS STANDARD

ATIS-0700048

Study of SHAKEN Impacts on 9-1-1 Calls and Callback Calls

TECHNICAL REPORT

Notice of Disclaimer & Limitation of Liability

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

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

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

ATIS-0700048, *Study of SHAKEN Impacts on 9-1-1 Calls and Callback Calls*

Published by

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

ATIS-0700048

ATIS Technical Report on

Study of SHAKEN Impacts on 9-1-1 Calls and Callback Calls

Alliance for Telecommunications Industry Solutions

Approved April 16, 2021

Abstract

This Technical Report studies the impacts of applying STIR/SHAKEN Caller Identity authentication and verification, as well as Resource-Priority header and SIP Priority header signing to 9-1-1 and callback calls.

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.

This Technical Report was developed jointly between ESIF, PTSC, and WTSC.

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

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

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:

R. Muscat, ESIF Chair (Bexar Metro 911)
D. Morkunas, ESIF First Vice Chair (Intrado)
J. Torres, ESIF Second Vice Chair (Verizon Wireless)

M. Dolly, PTSC Chair (AT&T)
V. Shaikh, PTSC Vice-Chair (Perspecta Labs)

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

T. Reese, Technical Editor (Ericsson)

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

Table of Contents

Table of Figures

ATIS Standard on –

Study of SHAKEN Impacts on 9-1-1 Calls and Callback Calls

1 Scope, Purpose, & Application

1.1 Scope

The Scope of this Technical Report is an analysis of the impacts of applying Secure Telephone Identity Revisited (STIR), as specified in RFC 8224 *Authenticated Identity Management in the Session Initiation Protocol (SIP)* [Ref 1] and Signature-based Handling of Asserted Information Using toKENs (SHAKEN), as specified in ATIS-1000074-E [Ref 2], *Errata on ATIS Standard on Signature-based Handling of Asserted information using toKENs (SHAKEN).* to 9-1-1 calls and callback calls. This Technical Report will also analyze the impacts of applying Resource-Priority Header (RPH) and SIP Priority header signing and verification to 9-1-1 calls and callback calls.

1.2 Purpose

This Technical Report is a study that analyzes the impacts on IP Multimedia Subsystem (IMS) originating networks of applying STIR/SHAKEN Caller Identity authentication and verification, and RPH and SIP Priority header signing/verification to 9-1-1 calls and callback calls to prevent malicious spoofing of Caller Identity, RPH, and SIP Priority header information. In particular, this study focuses on the identification of impacts to ATIS-0700015, *ATIS Standard for Implementation of 3GPP Common IMS Emergency Procedures for IMS Origination and ESInet/Legacy Selective Router Termination* [Ref 3].

1.3 Application

This Technical Report applies to emergency (9-1-1) calls originated in, and callback calls received by, IMS networks in North America to assist in the detection and mitigation of Caller Identity, and where applicable, RPH and SIP Priority header spoofing. This technical report is based on the SHAKEN procedures specified in ATIS-1000074-E, *Errata on ATIS Standard on Signature-based Handling of Asserted information using toKENs (SHAKEN)* [Ref 2].

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]: IETF RFC 8224, *Authenticated Identity Management in the Session Initiation Protocol (SIP)*.[1]

[Ref 2]: ATIS-1000074-E, *Errata on ATIS Standard on Signature-based Handling of Asserted information using toKENs (SHAKEN).*[2]

[Ref 3]: ATIS-0700015, *ATIS Standard for Implementation of 3GPP Common IMS Emergency Procedures for IMS Origination and ESInet/Legacy Selective Router Termination*.[2]

[Ref 4]: ATIS-1000072, *Analysis of Mitigation Techniques for Calling Party Spoofing*.[2]

[Ref 5]: NENA-STA-010.3, NENA i3 Standard for NG9-1-1 (to be issued).[3]

[Ref 6]: IETF Internet Draft draft-ietf-stir-rph-emergency-services-04, *Assertion Values for a Resource Priority Header Claim and a SIP Priority Header Claim in Support of Emergency Services Networks*.[1]

[Ref 7]: IETF RFC 7090, *Public Safety Answering Point (PSAP) Callback*.[1]

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

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

[3] This document is available from the National Emergency Number Association (NENA) at: < www.nena.org >.

[Ref 8]: 3GPP TS 24.229, *3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3* (Release 16).[4]

[Ref 9]: IETF RFC 8225, *PASSporT: Personal Assertion Token*.[1]

[Ref 10]: IETF RFC 8226, Secure Telephone Identity Credentials: Certificates.[1]

[Ref 11]: IETF RFC 8443, *Personal Assertion Token (PASSporT) Extension for Resource Priority Authorization*.[1]

[Ref 12]: ATIS-1000081, *ATIS Technical Report on a Framework for Display of Verified Caller ID*.[2]

[Ref 13]: IETF RFC 7378, *Trustworthy Location*.[1]

[Ref 14]: IETF RFC 7230, *Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing*.[1]

[Ref 15]: Task Force on Optimal PSAP Architecture (TFOPA) Working Group 1: *Optimal Cybersecurity Approach for PSAPs*, Final Report, dated December 10, 2015.[5]

[Ref 16]: ATIS-0500032, *Standard for Implementation of an IMS-based NG9-1-1 Service Architecture.*[2]

[Ref 17]: ATIS-0500036, *ATIS Standard for IMS-based Next Generation Emergency Services Network Interconnection.*[2]

[Ref 18]: 3GPP TS 23.167, *IP Multimedia Subsystem (IMS) emergency sessions.*[4]

[Ref 19]: ATIS/TIA J-STD-036-C-2, *Addendum to J-STD-036-C, Enhanced Wireless 9-1-1 Phase II.*[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

Attestation: This is the declaration made by a network operator that the party placing a particular call is authorized to represent themselves by a particular caller identity (see ATIS-1000074-E [Ref 2] for specific details).

Caller Identity: The originating or calling party telephone number used to identify the caller carried either in the P-Asserted Identity or From header.

Resource-Priority Header (RPH): A SIP header field that may be used by SIP user agents, including Public Switched Telephone Network (PSTN) gateways and terminals, and SIP proxy servers to influence their treatment of SIP requests, including the priority afforded to PSTN calls.

Priority Header: A SIP header field that is used to mark callback calls to increase the chances of reaching the emergency caller by allowing networks to use that marking to apply preferential treatment to those calls. See RFC 7090 [Ref 7] for further details.

3.2 Acronyms & Abbreviations

3GPP	Third Generation Partnership Project
ATIS	Alliance for Telecommunications Industry Solutions
BCF	Border Control Function
CN	Core Network
CPE	Customer Premises Equipment
CSCF	Call Session Control Function
CVT	Call Validation Treatment
DTMF	Dual Tone Multi Frequency

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

[5] This document is available from the Federal Communications Commission (FCC) at:
< https://transition.fcc.gov/pshs/911/TFOPA/TFOPA_WG1_FINAL_Report-121015.pdf >

ECRF	Emergency Call Routing Function
E-CSCF	Emergency Call Session Control Function
ESIF	Emergency Services Interconnection Forum
ESInet	Emergency Services IP network
ESN	Electronic Serial Number
ESRP	Emergency Service Routing Proxy
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IBCF	Interconnection Border Control Function
IETF	Internet Engineering Task Force
IM	IP Multimedia
IMEI	International Mobile Equipment Identity
IMS	IP Multimedia Subsystem
IP	Internet Protocol
JSON	JavaScript Object Notation
LoST	Location to Service Translation
LRF	Location Retrieval Function
NENA	National Emergency Number Association
NG	Next Generation
NG9-1-1	Next Generation 9-1-1
NGCS	Next Generation 9-1-1 Core Services
NGN PS	Next Generation Network Priority Service
NNI	Network-to-Network Interface
NS/EP	National Security / Emergency Preparedness
OCIF	Outbound Call Interface Function
OSP	Originating Service Provider
PASSporT	Personal Assertion Token
P-CSCF	Proxy Call Session Control Function
PIDF-LO	Presence Information Data Format – Location Object
PSTN	Public Switched Telephone Network
PTSC	Packet Technologies and Systems Committee
PSAP	Public Safety Access Point
RDF	Routing Determination Function
RPH	Resource-Priority Header
S-CSCF	Serving Call Session Control Function
SHAKEN	Signature-based Handling of Asserted information using toKENs
SIP	Session Initiation Protocol
SKS	Secure Key Store
STI	Secure Telephone Identity
STI-AS	Secure Telephone Identity Authentication Service
STI-CR	Secure Telephone Identity Certificate Repository
STIR	Secure Telephone Identity Revisited
STI-VS	Secure Telephone Identity Verification Service
TDOS	Telephony Denial of Service

TLS	Transport Layer Security
TN	Telephone Number
UA	User Agent
UE	User Equipment
URI	Uniform Resource Identifier
UUID	Universally Unique Identifier
VoIP	Voice over Internet Protocol
WTSC	Wireless Technologies and Systems Committee

4 Background

Illegitimate Caller Identity spoofing is a growing concern for North American telephone service providers and their customers. The Signature-based Handling of Asserted information using toKENs (SHAKEN) framework, as specified in ATIS-1000074-E [Ref 2], is intended to guide telephone service providers in using Secure Telephone Identity (STI) technologies to assist in the validation of legitimate calls and the mitigation of illegitimate spoofing of telephone identities on Internet Protocol (IP)-based service provider voice networks. The SHAKEN framework provides a general architecture to support service provider authentication and verification services based on the protocols defined in the Internet Engineering Task Force (IETF) Secure Telephone Identity Revisited (STIR) Working Group. Using the mechanisms defined in the STIR/SHAKEN standards, calls traveling through interconnected carrier networks have the legitimacy of their Caller Identity evaluated and, if asserted, "signed" as legitimate by the originating carrier. The terminating carrier performs validation checks against the signed Caller Identity before the calls are delivered to called users, allowing an indication to be provided to the called party regarding the legitimacy of the Caller Identity. Telecom operators are currently deploying robocalling mitigation solutions based on the SHAKEN framework defined in ATIS-1000074-E [Ref 2], the STIR protocols specified in RFC 8224 [Ref 1] and RFC 8225 [Ref 9], and the use of STI-related X.509-based certificates, as described in RFC 8226 [Ref 10].

There is value in applying the SHAKEN authentication and verification services and associated protocols to 9-1-1 calls and 9-1-1 callback calls. For emergency (9-1-1) originations, interactions between originating network elements and the SHAKEN authentication service to support Caller Identity assertion must be defined, as well as interactions between elements of the NG9-1-1 Emergency Services Network and the SHAKEN verification service, so that verification status information, indicating the “trustworthiness” of the caller identification (e.g., callback number) information, can be delivered to Public Safety Answering Points (PSAPs) along with the callback number. Additionally, interactions with the SHAKEN architecture and procedures must also be specified to address caller authentication associated with callback calls that are routed via an NG9-1-1 Emergency Services Network. Callback calls that have a Caller Identity that can be authenticated by the NG9-1-1 Emergency Services Network and verified by the emergency caller’s home network will have a higher chance of completing to the called party, which is an important feature for emergency callbacks.

In addition to Caller Identity authentication/verification, 9-1-1 calls and callback calls may also be subject to Resource-Priority Header (RPH) signing. Since the SIP signaling associated with 9-1-1 originations and callback calls includes an RPH, there is concern that the SIP RPH field could be spoofed and abused by bad actors, impacting the processing of 9-1-1/callback calls. In the context of 9-1-1 calls, signing the RPH would allow an originating service provider to assert that they recognize the call as an emergency (9-1-1) origination and that they populated the RPH. A signed RPH would also convey to the Emergency Services Network provider that they can trust that the RPH was populated by the originating service provider, as opposed to being inserted by a threat agent. This information could subsequently be conveyed to the PSAP, possibly via new ‘verstat’ values or other data.

In the context of callback calls, a signed RPH would indicate that the Emergency Services Network provider asserts that they recognize the call is a callback call and as such that an RPH value in the ‘esnet’ namespace is appropriate. It would also indicate to the emergency caller’s service provider that they can trust that the RPH was populated by the Emergency Services Network provider, as opposed to being inserted by a threat agent. In addition, IETF RFC 7090 [Ref 7] describes the use of the SIP Priority header field with the value "psap-callback" to mark callback calls to allow special network handling of the call, such as bypassing services that might preclude the call from completing. There is no protection against misuse of the SIP Priority field and because, as described in RFC 7090 [Ref 7], the SIP Priority header field may affect routing, it is desirable to protect it from modification. Home network providers serving emergency callers will benefit from knowing whether the Priority header accompanying a callback call can be trusted before applying special processing or routing to such calls.

IETF RFC 8443 [Ref 11] extends the Personal Assertion Token (PASSporT) specification defined in RFC 8225 [Ref 9] to allow the inclusion of cryptographically signed assertions for the values populated in the SIP RPH. The SIP RPH may be used to influence the prioritization of network resources that support communications sessions (e.g., in times of network congestion). Like Caller Identity information, the RPH field could be spoofed in a Telephony Denial of Service (TDOS) attack on the PSAP. RFC 8443 [Ref 11] supports PASSporT extensions that will allow the cryptographic signing of the SIP RPH and the conveyance of the signed SIP RPH. A signed SIP RPH will allow a receiving entity (including entities located in different network domains/boundaries) to verify the assertion of information in the SIP RPH, providing assurance that the information has not been spoofed or compromised. In the context of emergency (9-1-1) calling, the extension to the PASSporT to assert the use of an RPH value in the ‘esnet’ namespace will be in addition to the PASSporT object that is used to assert the Caller Identity. Specifically, assertion of the information in the RPH will involve the inclusion of a “ppt” extension with an “rph” claim in the PASSporT. According to RFC 8443 [Ref 11], the "rph" claim will provide an assertion of the information in the SIP RPH. The details of the syntax to be used with an "rph" claim for a SIP RPH that is associated with an emergency (9-1-1) origination, as well as an RPH PASSporT extension that includes an “rph” claim for a SIP RPH and an “sph” claim for a SIP Priority header associated with a callback call are specified in draft-ietf-stir-rph-emergency-services-04 [Ref 6].

After the header and the RPH-related claims PASSporT objects associated with a 9-1-1 call have been constructed, their signature is expected to be generated by the Originating Service Provider. A Service Provider can use the same certificates for signing SIP RPH as they use for Telephone Number (TN) signing but is not required to do so.

5 Assumptions

The following are assumptions regarding the application of SHAKEN to 9-1-1 calls and callback calls that are used in the analysis contained within this Technical Report.

1. The Request URI associated with an emergency (9-1-1) origination will contain an sos service URN; the To header associated with an emergency origination will either contain an sos service URN or the digits “911” expressed as a Uniform Resource Identifier (URI).
2. A Resource-Priority Header (RPH) in the ‘esnet’ namespace may or may not be associated with an emergency origination by the Proxy Call Session Control Function (P-CSCF) in the originating IMS network based on local policy.
3. Caller Identity assertion/authentication and/or rph signing will be performed by the originating network after it has been determined that the emergency call is to be routed to a Next Generation (NG) Emergency Services Network.
4. The NG Emergency Services Network will be responsible for performing verification of PASSporT information received with an emergency call.
5. Analytics (via the Call Validation Treatment [CVT] function defined in ATIS-1000074-E [Ref 2]) may be applied to an emergency origination based on local policy and agreements between the 9-1-1 Authority and the analytics/CVT provider.
6. Verstat and possibly other analytics-based information will be delivered to the PSAP with the emergency call and will be displayed to the PSAP in a consistent way.
7. Attestation information, if received by the NG9-1-1 Emergency Services Network, will be delivered to the PSAP with the emergency call.
8. The originating network provider will be notified by the NG Emergency Services Network if verification fails, as described in Clause 5.3.2 of ATIS-1000074-E [Ref 2].
9. Callback calls routed via the NG Emergency Services Network will be marked as “psap-callback” and will contain an RPH with a value of “esnet.0”.
10. The NG Emergency Services Network will be responsible for performing Caller Identity attestation/authentication and RPH and SIP Priority header signing on callback calls.
11. Privacy of Caller Identity information associated with callback calls will be supported/preserved.
12. Callback calls will use normal routing (i.e., via the emergency caller’s home network) to the network that is serving the emergency caller.
13. Verification of Caller Identity/RPH/SIP Priority header signing will be performed by the terminating home network for the callback call.

14. Verstat information associated with the callback call will be delivered to the emergency caller's User Equipment (UE).

    Note: What gets displayed to the user is not standardized and is dependent on how the user interface between the device and the user is implemented. See ATIS-1000081 [Ref 12] for guidelines regarding the display of verified Caller Identity information.

15. A Service Provider can use the same certificates for signing SIP RPH/Priority header as they use for TN signing, but is not required to do so.
16. SIP RPH signing does not change or modify 9-1-1/callback call processing, signaling and routing procedures; it simply provides a security tool for transit and receiving providers to determine if the SIP RPH is trusted.
17. If verification of the signed Caller Identity or SIP RPH associated with a 9-1-1 origination fails, the 9-1-1 call will be delivered to the PSAP with Caller Identity and SIP RPH, along with the results of the Caller Identity and RPH verification.

    Note: The mechanism for communicating a 'verstat' to convey RPH verification success/failure in a SIP INVITE message is for further study.

18. If validation of the signed Caller Identity or SIP RPH/Priority header associated with a callback call fails, terminating Service Provider local policy will determine terminating call processing, such as whether the call should be delivered with Caller Identity and/or SIP RPH and Priority header information intact. Note that if the call proceeds, a verstat parameter will be included in the associated SIP signaling. Further study is required to determine the mechanism for conveying SIP RPH/Priority header verification status in SIP signaling.
19. Signing of Caller Identity is separate from SIP RPH/Priority header signing. Separate SIP Identity headers are used for SIP RPH/Priority header signing and Caller Identity signing.

6 Use/Threat Cases

This clause describes some example threat cases associated with emergency (9-1-1) call originations that involve the spoofing of key signaling information (e.g., Caller Identity information, Resource-Priority Headers) and that might be addressed through the use of mitigation techniques such as SHAKEN and Resource-Priority Header signing. Note that these threat cases are based on Appendix 1 of the Task Force on Optimal PSAP Architecture (TFOPA) Working Group 1 Report on *Optimal Cybersecurity Approach for PSAPs* [Ref 15].

6.1 Telephony Denial of Service (TDOS) Attack

Short Description

A "bad actor" orchestrates an attack in which a large number of calls are made to 9-1-1. The calls used in the attacks use a spoofed Caller Identity, potentially changing the Caller Identity on every call to avoid detection. The objective of the attack is to tie up resources within the PSAP, preventing the handling of legitimate incoming calls and/or the making of outgoing calls. The audio content of the calls may include Dual Tone Multi Frequency (DTMF) patterns, white noise, or silence (which could be construed as a "silent call" from a disabled user, or as a technical problem).

Actors

Bob is the "bad actor" whose has orchestrated the attack.

PSAP1 is the NG PSAP that is compromised by the attack.

Pre-Conditions

Bob arranges for a large number of calls to be made to the target phone number(s), using a variety of spoofed Caller Identities.

Post-Conditions

The PSAP network slows and ultimately experiences a loss of communications.

If other PSAPs in the area are similarly affected, transfer of call taking capability may also become impossible.

The PSAP will recover when the attack ceases (at the discretion of the orchestrator) or as a result of pre-planned mitigation and recovery actions being invoked.

Example Flow

1. Bob originates multiple emergency calls from the same or nearby locations, using a different Caller Identity for each call. His call requests are forwarded to the originating network.
2. The originating network associates a callback number, an appropriate RPH value, and location information with each call.
3. The originating network performs location-based routing of each 9-1-1 call and determines that the call is to be routed via an NG9-1-1 Emergency Services Network.
4. The originating network routes each call toward the NG9-1-1 Emergency Services Network, passing the callback number, RPH and location information (by-value or by-reference).
5. The NG9-1-1 Emergency Services Network applies location and policy-based routing to each 9-1-1 call and identifies NG PSAP1 as the target destination for the calls. (Note that policy-based routing may cause calls to be alternate routed to other PSAPs due to congestion conditions at PSAP1.)
6. The NG9-1-1 Emergency Services Network delivers each 9-1-1 call to NG PSAP1 with callback information, RPH, and location (by-value or by-reference).
7. PSAP1's call handling equipment processes the Caller Identity information (i.e., callback number), RPH, and location. If the location was received "by-reference", this processing will include initiation of a dereference request to obtain Bob's location information.
8. Calls are answered, with Bob's location information and callback information displayed on the call taker's Customer Premises Equipment (CPE) until PSAP call-taking queues fill as the number of 9-1-1 originations exceeds the number of available call takers. (Note that the call handling procedures at NG PSAP1 are further complicated if Bob's calls are delivered as "silent" calls.)

Alternate Flow

1. Bob originates multiple emergency calls from the same or nearby locations, using a different Caller Identity for each call. His call requests are forwarded to the originating network.
2. The origination network associates a callback number, an appropriate RPH value, and location information with the call.
3. The originating network associates an attestation level with the Caller Identity (i.e., callback number) based on the relationship that the Originating Service Provider (OSP) has with the caller and the ability of the OSP to recognize whether the Caller Identity is appropriate for that caller. Where neither the caller nor the Caller Identity is recognized, an attestation level of "C" is associated with the call. [Note: Attestation may happen either before or after call routing.]
4. The originating network performs location-based routing of each 9-1-1 call and determines that the call is to be routed via an NG9-1-1 Emergency Services Network.
5. Based on interactions with an Authentication Service, the Caller Identity and RPH associated with each 9-1-1 call are signed.
6. The originating network routes each call toward the NG9-1-1 Emergency Services Network, passing the signed callback number and RPH, and location information (by-value or by-reference).
7. The NG9-1-1 Emergency Services Network interacts with a Verification Service which performs verification of the signed Caller Identity and RPH associated with each call. In this example, the verification is successful.

8. The NG9-1-1 Emergency Services Network applies location and policy-based routing to each 9-1-1 call. (Note that policy-based routing may cause calls to be alternate routed to other PSAPs due to congestion conditions at PSAP1.)
9. The NG9-1-1 Emergency Services Network delivers 9-1-1 calls to NG PSAP1 with callback information (and associated verification status and attestation level), RPH (and associated verification status), and location (by-value or by-reference).
10. PSAP1's call handling equipment processes the Caller Identity information (i.e., callback number, verification status, attestation level), RPH (and verification status), and location. If the location was received "by-reference", this processing will include initiation of a dereference request to obtain Bob's location information.
11. Calls are answered, with Bob's location information and callback information (along with the verification status and attestation level) displayed on the call takers' CPE until PSAP call-taking queues fill as the number of 9-1-1 originations exceeds the number of available call takers.
12. Recognizing the large number of 9-1-1 calls being received with "C" level attestation, NG PSAP1 invokes attack mitigation procedures (while handling received calls per Operating Procedures). (Note that the call handling procedures at NG PSAP1 are further complicated if Bob's calls are delivered as "silent" calls.)

6.2 Swatting Attack

Short Description

Swatting is the act of causing the dispatch of an emergency response based on the false report of an ongoing critical incident. With the transition to NG9-1-1, this may be facilitated by directly providing false location information along with the call. As described in IETF RFC 7378 [Ref 13], location provided to PSAPs associated with calls from fixed devices (e.g., circuit-switched calls from landlines, or Voice over Internet Protocol [VoIP] services that only support emergency service calls from stationary devices), is determined from a lookup using the calling telephone number. As a result, for landlines or fixed VoIP, spoofing of Caller Identity can result in the PSAP incorrectly determining the caller's location. Ideally, a call taker at a PSAP should be able to assess, in real time, the level of trust that can be placed on the information provided within a call. Where real-time assessment is not possible, it is important to be able to determine the source of the call in a post-incident investigation, so as to enable law enforcement to conduct a criminal investigation. In this example, swatting is used to distract emergency services to a location that is a distance from the location of a criminal action (e.g., a bank robbery).

Actors

Bob is the "bad actor" who has orchestrated the swatting attack.

Carol is the call taker /dispatcher in NG PSAP1 that receives the swatting call(s).

Pre-Conditions

Bob initiates a 9-1-1 call using a spoofed Caller Identity and location.

Post-Conditions

Carol interprets the information presented to her and follows protocols for dispatch, dispatching appropriate services to the false location.

First Responders travel to the false location(s), leaving depleted resources available to respond to the location where the criminal action is taking place.

The arrival of First Responders at the false location(s) creates confusion at the false locations, possibly resulting in additional calls being generated to 9-1-1.

During the peak of the confusion, requests for emergency services begin to be received by NG PSAP1 related to Bob's actual crime.

Local resources for dispatch are not available or have limited availability, possibly causing NG PSAP1 to reach out for mutual aid.

Example Flow

1. Bob originates a 9-1-1 call with a spoofed Caller Identity and spoofed location. His call request is forwarded to the originating network.
2. The originating network associates a callback number, an appropriate RPH value, and location information with the call.
3. The originating network performs location-based routing of each 9-1-1 call and determines that the call is to be routed via an NG9-1-1 Emergency Services Network.
4. The originating network routes the call toward the NG9-1-1 Emergency Services Network, passing the callback number, RPH and location information (by-value or by-reference).
5. The NG9-1-1 Emergency Services Network applies location and policy-based routing to the 9-1-1 call and determines that the call is destined for NG PSAP1.
6. The NG9-1-1 Emergency Services Network delivers the 9-1-1 call to NG PSAP1, with callback information, RPH, and location (by-value or by-reference).
7. Carol answers the call.
8. In parallel, Carol's call handling equipment processes the Caller Identity information (i.e., callback number), RPH, and location. If the location was received "by-reference", this processing will include initiation of a dereference request to obtain Bob's location information.
9. Bob's location information and callback information are displayed on Carol's CPE.
10. Carol initiates the dispatch of emergency personnel to the spoofed location provided with the 9-1-1 call (and confirmed by the "bad actor").

Alternate Flow

1. Bob originates a 9-1-1 call with a spoofed Caller Identity and spoofed location. His call request is forwarded to the originating network.
2. The originating network associates a callback number, an appropriate RPH value, and location information with the call.
3. The originating network associates an attestation level with the Caller Identity (i.e., callback number) based on the relationship that the OSP has with the caller and the ability of the OSP to recognize whether the Caller Identity is appropriate for that caller. Where neither the caller nor the Caller Identity is recognized, an attestation level of "C" is associated with the call. [Note: Attestation may happen either before or after call routing.]
4. The originating network performs location-based routing of each 9-1-1 call and determines that the call is to be routed via an NG9-1-1 Emergency Services Network.
5. Based on interactions with an Authentication Service, the Caller Identity and RPH associated with the 9-1-1 call are signed. This example also assumes that it is possible to sign and associate something comparable to an attestation level with the location information.[6]
6. The originating network routes the call toward the NG9-1-1 Emergency Services Network, passing the signed callback number, RPH, and location information (by-value or by-reference).

[6] See Clause 11.3 for further discussion regarding the need to define a mechanism by which the trustworthiness of location information can be asserted/signed and verified.

7. The NG9-1-1 Emergency Services Network interacts with a Verification Service which performs verification of the signed Caller Identity, RPH, and location associated with the call. In this example, the verification is successful.
8. The NG9-1-1 Emergency Services Network applies location and policy-based routing to the 9-1-1 call and determines that the call is destined for NG PSAP1.
9. The NG9-1-1 Emergency Services Network delivers 9-1-1 calls to NG PSAP1 with callback information (and associated verification status and attestation level), RPH (and associated verification status), and location (by-value or by-reference, with associated verification status and “attestation” level).
10. PSAP1’s call handling equipment processes the Caller Identity information (i.e., callback number, verification status, attestation level), RPH (and verification status), and location (and verification status and “attestation” level). If the location was received “by-reference”, this processing will include initiation of a dereference request to obtain Bob’s location information.
11. Carol answers the call.
12. Bob’s location information (including verification status and “attestation” level) and callback information (along with the verification status and attestation level) are displayed on the call takers’ CPE.
13. Recognizing that the Caller Identity associated with the 9-1-1 call has a “C” level attestation, and that the “attestation” level associated with the location also indicates potential spoofing, Carol performs further checks on the Caller Identity and location before dispatching emergency personnel and/or warns the first responders of the questionable nature of the Caller Identity and location.

7 Standards Relevant to SHAKEN and 9-1-1/Callback Calls

7.1 ATIS-1000074-E

ATIS-1000074-E [Ref 2] provides a framework and guidance on how to utilize Secure Telephone Identity (STI) technologies to support the validation of legitimate calls in an effort to mitigate illegitimate spoofing of telephone identities on VoIP networks. ATIS-1000074-E [Ref 2] focuses on the format of STI claims, the mapping of these claims to SIP signaling, and support for service provider authentication and verification services. Using the mechanisms defined in ATIS-1000074-E [Ref 2], calls traveling through interconnected carrier networks can have the legitimacy of their Caller Identity evaluated and, if asserted, “signed” as legitimate by the originating carrier. The terminating carrier performs validation checks against the signed Caller Identity before the calls are delivered to called users, allowing the terminating carrier of the party receiving the call to provide an indication to the called party of the legitimacy of the Caller Identity. ATIS-1000074-E [Ref 2] does not consider Caller Identity authentication associated with emergency (i.e., 9-1-1) calls or PSAP callback calls. This is a topic of ongoing work within the IP-NNI Task Force.

7.2 ATIS-0700015

ATIS developed ATIS-0700015, *ATIS Standard for Implementation of 3GPP Common IMS Emergency Procedures for IMS Origination and ESInet/Legacy Selective Router Termination* [Ref 3] to define and adapt as necessary 3GPP common IMS emergency procedures for applicability in North America. This standard supports emergency communications originating from an IMS subscriber (fixed, nomadic, or mobile) and delivered to an Emergency Services IP network (ESInet) or to a legacy Selective Router. The potential interactions between IMS functional elements in the ATIS-0700015 [Ref 3] architecture and the SHAKEN infrastructure must be considered to fully support Caller Identity assertion and verification associated with emergency calls, as well as verification of Caller Identity information presented with callback calls. In the context of emergency services, caller authentication/verification associated with callback calls is necessary to ensure that the callback calls receive the desired call treatment and provide the best chance of being answered by the intended party. This study assesses the impacts on the ATIS-0700015 [Ref 3] architecture of supporting the application of SHAKEN Caller Identity authentication procedures and RPH signing to emergency (9-1-1) calls and SHAKEN Caller Identity as well as SIP RPH/Priority header verification procedures to callback calls.

7.3 ATIS-0500032

ATIS-0500032, *ATIS Standard for Implementation of an IMS-based NG9-1-1 Service Architecture* [Ref 16], applies IMS architecture concepts to Next Generation 9-1-1 (NG9-1-1) networks and defines an IMS-based NG9-1-1 Service Architecture that includes an IMS NG9-1-1 Emergency Services Network and additional gateway functional elements adopted from the National Emergency Number Association (NENA) i3 architecture, to support the delivery of emergency calls to legacy and NG9-1-1/i3 PSAPs. Updates to ATIS-0500032 have been proposed to address the impacts on the IMS-based NG9-1-1 Emergency Services Network of supporting procedures to verify caller identification (i.e., callback number) and RPH information associated with 9-1-1 originations, as well as the delivery of Caller Identity attestation and verification status information, and RPH verification status information to PSAPs. Interactions between IMS-based NG9-1-1 Emergency Services Networks and the SHAKEN architecture and procedures are also necessary to support caller authentication, as well as SIP RPH/Priority header signing associated with callback calls that are routed via the NG9-1-1 Emergency Services Network toward the emergency caller. Work is ongoing to fully assess the impacts on ATIS-0500032 to support the application of STIR/SHAKEN procedures to emergency (9-1-1) calls and callback calls.

7.4 ATIS-0500036

ATIS-0500036, *ATIS Standard for IMS-based Next Generation Emergency Services Network Interconnection* [Ref 17], defines the architecture and protocols to enable the interconnection of North American IMS-based NG9-1-1 emergency services networks with other legacy and Next Generation Emergency Services Networks deployed in North America to support the delivery of initial and transferred emergency calls. Further study is needed to assess the impacts on SHAKEN verification procedures associated with alternate-routed or transferred 9-1-1 calls that are passed between NG9-1-1 Emergency Services Networks.

7.5 3GPP TS 23.167

3GPP TS 23.167, *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS) emergency sessions* [Ref 18], defines the stage 2 service description for emergency services in the IP Multimedia Core Network Subsystem (IMS). TS 23.167 does not currently address requirements related to Caller Identity spoofing mitigation techniques, like those supported using STIR/SHAKEN, or signing/verification of the content of the Resource-Priority header or Priority header. Modifications would be needed to the architectural principles described in Clause 4.1 to allow for Caller Identity assertion and verification associated with emergency calls and callback calls, as well as signing/verification of RPH/Priority header information in emergency and callback calls to prevent spoofing of Caller Identity and misuse of resource priority and priority information, based on local regulation. In addition, Clauses 7.3, 7.4, and K.2.2 would need to be modified to allow a P-CSCF to perform attestation of Caller Identity for an emergency session, if configured through operator policies. Modifications to Clause 6.2.12 would also be needed to allow an exit Interconnection Border Control Function (IBCF) in an IMS originating network, if configured through operator policies, to invoke an Application Server for the signing of Caller Identity and Resource-Priority header information, if available in the incoming request, and to include the signed information in the outgoing request. This would include scenarios in which a non-dialable callback number has been associated with the emergency request by the Emergency Call Session Control Function (E-CSCF), as described in Clause 7.4. The IBCF in an emergency caller's home network may also, if configured through operator policies, invoke an Application Server to perform verification of signed Caller Identity, Resource-Priority Header content, and SIP Priority header content associated with callback calls.

7.6 3GPP TS 23.228

3GPP TS 23.228, *3rd Generation Partnership Project; Technical Specification Group Core Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2* [Ref 19], defines the Stage 2 service description for the IP Multimedia Core Network Subsystem (IMS), which includes the elements necessary to support IP Multimedia (IM) services. 3GPP TS 23.228 addresses authentication and verification of Caller Identity in the context of non-emergency calls. Specifically, Clause 4.6.3 of 3GPP TS 23.228 supports the attestation of the identity of an originating subscriber by a Serving Call Session Control Function (S-CSCF), possibly via interactions with an Application Server, if configured through operator policies. In addition, Clause 4.14 of 3GPP TS 23.228 describes a mechanism by which an exit IBCF in an originating network, if configured through operator policies, can invoke an Application Server for the signing of attestation and identity information if available in the incoming request. The

IBCF then includes the signed information in the outgoing request. In addition, for a terminating session arriving at an entry IBCF without attestation information, the IBCF may add, if configured through policies, gateway attestation information based on the network from which the request was received. An entry IBCF that receives a terminating session with signed attestation information may, if configured through policies, invoke an Application Server for signature verification. Since 3GPP TS 23.228 addresses emergency sessions by reference to 3GPP TS 23.167, it may not be appropriate to update this document to specifically address Caller Identity signing/verification or Resource-Priority Header signing/verification in the context of emergency calling. Consideration may be given to adding procedures to 3GPP TS 23.228 to support Resource-Priority Header signing in the context of priority services, however that is outside the scope of this ATIS study.

7.7 3GPP TS 24.229

3GPP TS 24.229, *3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3* [Ref 8], defines a call control protocol for use in the IP IM Core Network (CN) subsystem based on the Session Initiation Protocol (SIP), and the associated Session Description Protocol (SDP). 3GPP TS 24.229 [Ref 8] addresses calling number verification using signature verification and attestation information, as applicable to non-emergency calls. In Clause 5.10.3.2, TS 24.229 [Ref 8] describes procedures at an entry IBCF that supports calling number verification using signature verification and attestation information. TS 24.229 [Ref 8] also defines the Attestation-Info and Origination-Id header fields used in the calling number authentication process. TS 24.229 [Ref 8] does not currently address the application of calling number verification associated with emergency originations or callback calls, nor does it address RPH signing/verification in the context of emergency originations or callback calls, or SIP Priority header signing in the context of callback calls. Further study is needed to assess the impacts on TS 24.229 [Ref 8] of applying calling number signing/verification protocol procedures to emergency originations (including scenarios where a non-dialable callback number is present, as described in Clause 5.11.2) and callback calls. In addition, potential impacts to TS 24.229 [Ref 8] to address RPH signing/verification in the context of emergency calls, and RPH/Priority header signing/verification in the context of callback calls, must also be identified.

8 Architecture

8.1 Reference Architecture for Emergency (9-1-1) Originations

Figure 8.1 shows one reference architecture for Caller Identity authentication and SIP RPH signing in the context of emergency originations. This architecture assumes the calling number authentication/verification architecture supported by 3GPP TS 24.229 [Ref 8] and TS 23.228, where an IBCF in an originating network, if configured through operator policies, invokes an Application Server via the Ms reference point for the signing and attestation of identity information, if available in an incoming request. The IBCF then includes the signed information in the outgoing request. In Figure 8-1, the emergency call is originated from service provider A's network that performs the authentication service and delivered to i3 ESInet /Next Generation 9-1-1 Core Services (NGCS) Provider 1's network, which performs the verification service.

As described in Clause V.2.1 of 3GPP TS 24.229 [Ref 8], the Ms reference point is used to request the signing of an Identity header field or to request verification of a signed identity in an Identity header field. The protocol to be used on the Ms Reference Point is HTTP 1.1, as specified in RFC 7230 [Ref 14][7].

[7] Note that Annex V of 3GPP TS 24.229 [Ref 8] identifies RFC 2616 as the reference for HTTP 1.1. RFC 2616 has been obsoleted by RFC 7230 [Ref 14]

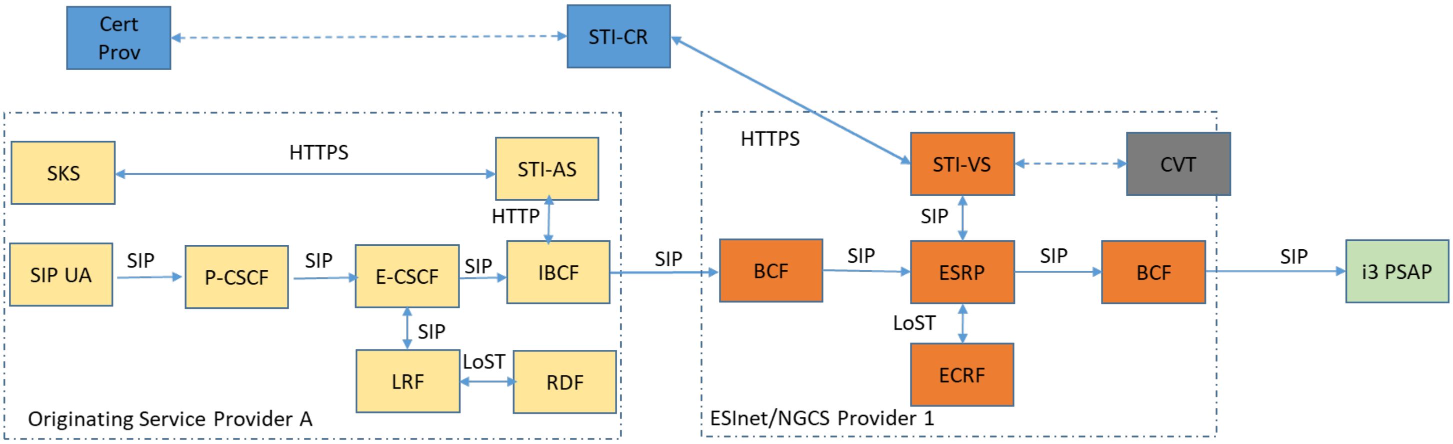

Figure 8.1: Emergency Services Initial Call Example

- Proxy Call Session Control Function (P-CSCF) – This component receives the emergency session establishment request from the UE, detects that it is an emergency session request, and forwards it to the E-CSCF. A P-CSCF operating in an Originating Service Provider network that supports calling number authentication and RPH signing may, based on local policy, be responsible for inserting attestation information related to the asserted Caller Identity and populating the RPH in a SIP INVITE associated with an emergency origination. According to 3GPP TS 24.229 [Ref 8], when a node performs attestation of an identity in an incoming request or can attest the origin of the request, the node can inform a downstream node about what kind of attestation the node has performed. Based on local policy, if the P-CSCF is responsible for providing attestation information on the Caller Identity associated with an authenticated emergency call, the P-CSCF will insert a verstat parameter in the P-Asserted-Identity header, an optional Attestation-Info header field in the SIP INVITE with a value of "A", "B" or "C", as defined in ATIS-1000074-E [Ref 2], associated with the Caller Identity, and an optional origination identifier [in the form of a Universally Unique Identifier (UUID)] in an Origination-Id header field. The P-CSCF may also populate a value of “esnet.1” in the RPH.

- Interconnection Border Control Function (IBCF) – This function is at the edge of the service provider network and represents the Network-to-Network Interface (NNI) or peering interconnection point between telephone service providers. It is the ingress and egress point for SIP calls between providers.

  In the context of an emergency (9-1-1) origination from an authenticated user, an exit IBCF will be responsible for sending an HTTP POST message containing two signingRequests over the Ms reference point to the STI-AS if a verstat parameter exists in the received P-Asserted-Identity header. The signingRequest associated with the Caller Identity will include an “attest” parameter that contains the attestation information and an “origid” based on local policy or received by the IBCF in Attestation-Info and Origination-Id headers respectively, as well as other PASSporT information (i.e., “orig”, “dest”, and iat). The signingRequest associated with the RPH will include an “rph” claim that contains an assertion of “ “esnet.1” associated with the “auth” key, along with the “orig”, “dest”, and “iat”. The exit IBCF will populate the assertion value in the signingRequest based on receipt of an RPH value of esnet.1.[8] The exit IBCF will populate Identity header fields in the outgoing SIP INVITE message based on the identityHeader parameters it receives in the HTTP signingResponses. The exit IBCF must remove the verstat from the From header or P-Asserted-Identity header prior to sending the SIP INVITE over the IP NNI to an NG9-1-1Emergency Services Network.

- Secure Telephone Identity Authentication Service (STI-AS) – The SIP application server that performs the function of the authentication service defined in RFC 8224 [Ref 1]. It should either itself be highly secured and contain the Secure Key Store (SKS) of secret private key(s) or have an authenticated, Transport Layer Security (TLS)-encrypted interface to the SKS that stores the secret private key(s) used to create PASSporT signatures.

[8] The HTTP interface used over the Ms interface will require enhancement to support the conveyance of the “rph” claim and associated assertion values.

In the context of emergency (9-1-1) originations, the STI-AS will receive an HTTP POST message from the IBCF that includes a signingRequest that contains the attestation information and PASSporT claims (i.e., “orig”, “dest”, iat and origid), as well as a signing request that contains an “rph” claim. The STI-AS determines through service provider-specific means the legitimacy of the content of the Caller Identity and the RPH field (i.e., the value in the “esnet” namespace), then securely requests its private key from the SKS. Upon receiving the private key from the SKS, the STI-AS signs and returns to the IBCF an Identity header field value for the Caller Identity and an Identity header field value for the RPH in JavaScript Object Notation (JSON) objects in signingResponse messages within an HTTP 200 OK.

- Secure Telephone Identity Verification Service (STI-VS) – The SIP application server that performs the function of the verification service defined in RFC 8224 [Ref 1]. It has a Hypertext Transfer Protocol Secure (HTTPS) interface to the Secure Telephone Identity Certificate Repository (STI-CR) that is referenced in the Identity header field to retrieve the provider public key certificate. Upon receiving a SIP INVITE message containing Identity headers associated with an emergency (9-1-1) origination from an ESRP in the i3 NG9-1-1 Emergency Services Network, the STI-VS retrieves the certificate referenced by the “x5u” field in the PASSporT protected header from the STI-CR. The STI-VS validates that the PASSporT information provided in the Identity headers contained in the SIP INVITE message includes all of the baseline claims, as well as the SHAKEN extension claims and “rph” claim. The STI-VS also follows the RFC 8224 [Ref 1]-defined verification procedures to check the corresponding date, originating identity and destination identities. The STI-VS will include verstat information (associated with the Caller Identity and with the RPH) in the SIP INVITE message returned to the ESRP to convey the results of the verification. The STI-VS must be invoked prior to terminating call processing associated with the emergency call. Note: The specific ‘verstat’ values associated with RPH signing verification success/failure are for further study.
- Call Validation Treatment (CVT) – This is a logical function that could be an application server function or a third party application for applying anti-spoofing mitigation techniques once the signature is positively or negatively verified. The CVT can also provide information in its response that indicates how the results of the verification should be displayed to the called user.
- SKS – The Secure Key Store is a logical highly secure element that stores secret private key(s) for the authentication service (STI-AS) to access.
- Certificate Provisioning Service – A logical service used to provision certificate(s) used for STI.
- Secure Telephone Identity Certificate Repository (STI-CR) – This represents the publicly accessible store for public key certificates. This should be an HTTPS web service that can be validated back to the owner of the public key certificate.
- Emergency Call Session Control Function (E-CSCF) – This is the IMS network entity that is responsible for routing emergency requests to a legacy or NG9-1-1 Emergency Services Network based on location information.
- Location Retrieval Function (LRF) - The LRF obtains location information for a UE and uses that location to acquire routing information for an emergency session from the Routing Determination Function (RDF).
- Routing Determination Function (RDF) – The RDF provides routing information for an emergency session based upon the location information and service URN in a request from the LRF. This routing information will designate a legacy Emergency Services Network or a NENA i3 ESInet/NGCS.
- Border Control Function (BCF) – This i3 functional element provides a secure entry into an i3 Emergency Services IP Network (ESInet) for emergency calls presented to the network. The BCF incorporates firewall, admission control, and may include anchoring of session and media as well as other security mechanisms to prevent deliberate or malicious attacks on PSAPs or other entities connected to the ESInet. As the first active SIP element in an i3 NG9-1-1 Emergency Services Network in the path of an emergency call, the BCF must add the Call Identifier, Incident Tracking Identifier, and a Resource-Priority header set to “esnet.1” (if not already present) to the SIP INVITE message associated with the emergency call. If a verstat parameter is present in the From or P-Asserted-Identity header of the received SIP INVITE, the BCF must remove it. The BCF forwards the SIP INVITE to the ESRP.
- Emergency Service Routing Proxy (ESRP) - An i3 functional element which is a SIP proxy server that selects the next hop routing within the ESInet based on location and policy. It is responsible for interacting with the STI-VS for verification of Caller Identity information and RPH information against the signatures.

The ESRP is expected to pass the received SIP INVITE message to the verification service before applying any call processing (e.g., location- and/or policy-based routing) to the call.

- Emergency Call Routing Function (ECRF) - A functional element in an i3 ESInet which is a Location to Service Translation (LoST) protocol server where location information (either civic address or geo-coordinates) and a Service URN serve as input to a mapping function that returns a URI used to route an emergency call toward the appropriate PSAP for the caller's location or towards a responder agency.

8.2 Reference Architecture for Callback Calls

Figure 8.2 shows one reference architecture for Caller Identity authentication and SIP RPH/Priority header signing in the context of callback calls. The architecture used for authenticating the Caller Identity and signing the SIP RPH and Priority header associated with callback calls assumes that an Outbound Call Interface Function (OCIF) in an i3 ESInet, if configured through operator policies, invokes Caller Identity authentication and RPH/Priority header signing by passing the SIP INVITE message associated with the callback call to the STI-AS. Specifically, an OCIF processing a SIP INVITE associated with a callback call will interact with the STI-AS to assert the telephone identity of the caller (i.e., a P-Asserted-Identity header field containing sip:TN@<psapdomain>;user=phone, where the TN is associated with the PSAP originating the callback call) and to request signing of the RPH value (i.e., esnet.0) and the SIP Priority header value (i.e., "psap-callback") included in the SIP INVITE message associated with the callback call. The OCIF will invoke the STI-AS for callback calls presented to it after call processing has completed, that is, after the target interconnected network has been determined to be an IP network.

Once the assertion and signing process is completed, the OCIF will receive the INVITE back from the STI-AS with two added SIP Identity header fields constructed per RFC 8224 [Ref 1], one associated with the Caller Identity and one associated with the RPH/SIP Priority header. After receiving the SIP INVITE from the STI-AS, the OCIF will route the call to the egress BCF. The egress BCF will then route the call over the NNI through the standard inter-domain routing configuration toward the entry IBCF associated with the emergency caller's home network. The home network will perform STI verification, assuming it supports such capabilities, and present the called party UE (i.e., the UE of the emergency caller) with an indication of the verification status of the calling telephone number and RPH/Priority header. Note that the architecture example illustrated below illustrates a scenario where the entry IBCF in the emergency caller's home network interacts with the STI-VS using an HTTP interface. As an alternative, the CSCF in the emergency caller's home network could use a SIP interface to interact with the STI-VS.

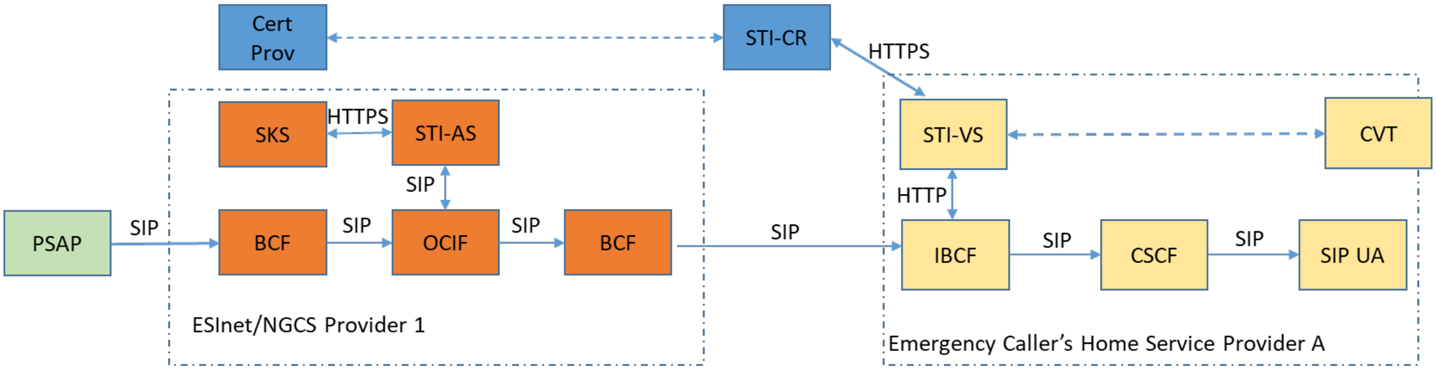

Figure 8.2: Emergency Services Callback Example

- Outbound Call Interface Function (OCIF) - Part of the NGCS that is responsible for handling calls originated by i3 PSAPs over their serving ESInet/NGCS. The OCIF is used to process callbacks as well as other outgoing calls that transit the ESInet (e.g., official calls from one Public Safety agency to another, perhaps on a different ESInet). It is responsible for interacting with the STI-AS for authentication/signing of Caller Identity information, RPH information, and SIP Priority header information.

- Secure Telephone Identity Authentication Service (STI-AS) – In the context of callback calls, the STI-AS will receive SIP INVITE messages associated with callback calls from an OCIF and will be responsible for determining, through service provider-specific means, the legitimacy of the telephone number identity, RPH, and SIP Priority header being used in the INVITE. The STI-AS is then responsible for cryptographically signing the PASSporT and adding Identity header fields and signatures (corresponding the Caller Identity and RPH/SIP Priority header) to the SIP INVITE that it returns to the OCIF.

- Interconnection Border Control Function (IBCF) – In the context of callback calls, the entry IBCF in the emergency caller's home network sends an HTTP verificationRequest over the Ms reference point to the STI-VS. The verificationRequest includes an identityHeader claim for each Identity header received, as well as the "to" parameter containing the destination identity from the To header, the "from" parameter containing the asserted identity from the From or P-Asserted-Identity, and a "time" parameter based on the Date header field in the incoming request. Upon receiving a verificationResponse from the STI-VS containing verstatValue parameters associated with each verified Identity header, the entry IBCF will populate the verstat information in the outgoing SIP INVITE message it sends to the Call Session Control Function (CSCF).

9 High-Level Call Flows

Figure 9.1 in Clause 9.1 illustrates a call flow based on the assumed reference architecture for Calling Identity authentication and SIP RPH signing in the context of emergency originations shown in Figure 8.1. Figure 9.2 in Clause 9.2 illustrates an emergency callback call flow based on the reference architecture shown in Figure 8.2.

9.1 Call Flow for Emergency Originations

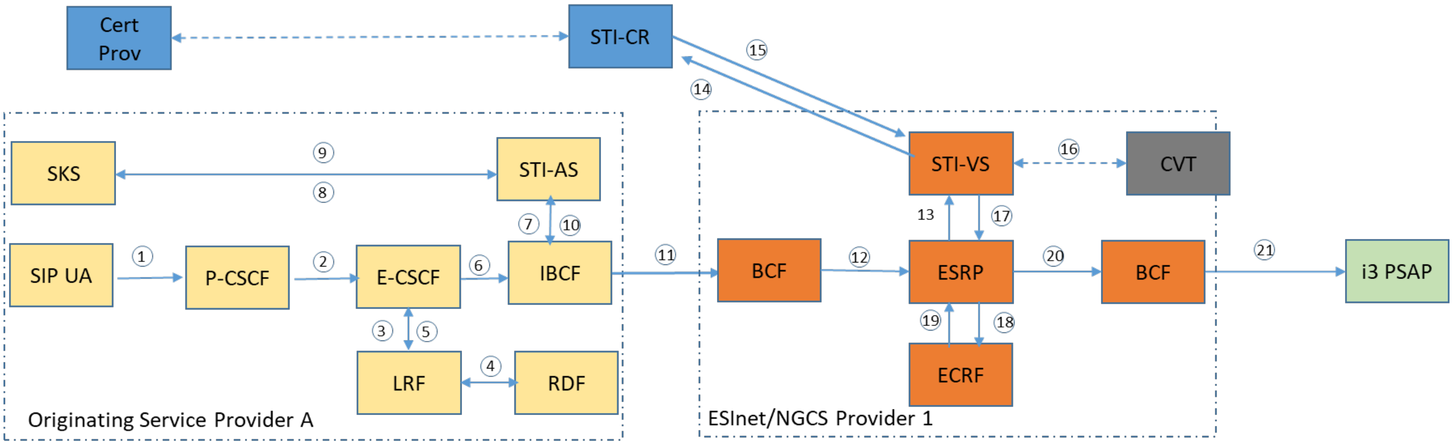

Figure 9.1: Emergency Services Initial Call Flow

1. The originating SIP User Agent (UA), which first REGISTERs and is authenticated to the P-CSCF, creates a SIP INVITE with a telephone number identity.
2. The P-CSCF in the originating network adds a P-Asserted-Identity header field asserting the Caller Identity of the originating SIP UA and an RPH with value "esnet.1". The P-CSCF passes the SIP INVITE to the E-CSCF. If supported by local policy, the P-CSCF will also insert a verstat parameter in the P-Asserted-Identity header, and optional Attestation-Info[9] and Origination-Id header fields in the SIP INVITE message for use by downstream calling identity authentication and verification processes.
3. The E-CSCF sends the INVITE to the LRF to determine routing instructions.
4. The LRF acquires location, if required, and queries the RDF for a routing URI.
5. The LRF returns the routing URI to the E-CSCF.
6. If the emergency call is destined to a NENA ESInet (i.e., not a legacy Selective Router), the E-CSCF forwards the emergency call to the exit IBCF.
7. The exit IBCF sends an HTTP POST message containing two signingRequests over the Ms reference point to the STI-AS. The signingRequest associated with the Caller Identity includes an "attest" parameter that

[9] The Attestation-Info header field in the SIP INVITE will contain a value of "A", "B" or "C", as defined in ATIS-1000074-E [Ref 2], as appropriate for the Caller Identity.

contains the attestation information received by the IBCF in an Attestation-Info parameter in the SIP INVITE, as well as other PASSporT information (i.e., "orig", "dest", iat and origid). The signingRequest associated with the RPH will include an "rph" claim that contains an "auth" key with an assertion of "esnet.1", along with the "orig", "dest", and "iat".[10] The IBCF will populate the assertion value in the signingRequest associated with the RPH based on the RPH value received in the incoming SIP INVITE message.

Note: The STI-AS must be invoked after originating call processing.

8. The STI-AS in the originating SP network (i.e., Service Provider A) first determines through service provider-specific means the legitimacy of the telephone number identity and RPH information being used in the INVITE. The STI-AS then securely requests its private key from the SKS.
9. The SKS provides the private key in the response, and the STI-AS signs the Caller Identity and RPH information provided in the "orig" and "rph" claims of the signingRequests.
10. The STI-AS returns signed identityHeader parameters associated with the Caller Identity and RPH information in signingResponses within an HTTP 200 OK message.
11. The IBCF uses the information returned in the identityHeader parameters to populate SIP Identity headers associated with the Caller Identity and the RPH in the SIP INVITE message. The IBCF removes any verstat information from the P-Asserted-Identity header or From header, if present, and routes the SIP INVITE over the NNI to the ingress BCF using standard inter-domain routing resolution.

Note: In support of Assumption #3 in Clause 5, an implementation option may allow the ECRF/LRF or IBCF to determine, based on the capabilities of the target Emergency Services Network, what information related to Caller Identity and RPH authentication will be forwarded to the interconnected network.

12. The ESInet ingress BCF receives the INVITE over the NNI and forwards it to the ESRP.[11]
13. The ESRP forwards the SIP INVITE message to the STI-VS.

Note: The STI-VS must be invoked before terminating call processing.

14. The terminating SP STI-VS uses the "x5u" field in the PASSporT Protected Header per RFC 8225 [Ref 9] to determine the STI-CR Uniform Resource Identifier (URI) and makes an HTTPS request to the STI-CR.
15. The STI-VS validates the certificate (see Clause 5.3.1 of ATIS-1000074-E [Ref 2] for details) and then extracts the public key. It constructs the RFC 8224 [Ref 1] format and uses the public key to verify the signature in the Identity header fields, which validate the Caller Identity and RPH field used when signing "orig" and "rph" claims at the originating service provider STI-AS.
16. The STI-VS may interact with the CVT based on local policy and agreements between the 9-1-1 Authority and the analytics/CVT provider. The CVT is an optional function that can be invoked to perform call spam analytics or other mitigation techniques and return a response related to what should be signaled to the user for a legitimate or illegitimate call. The CVT may be integrated in the service provider network or may be provided by a third party outside of the service provider network.
17. The STI-VS passes the INVITE back to the ESRP with appropriate indicators (i.e., "verstat" values and possibly other information that may be defined outside of this document).

Note: Provisional "verstat" values associated with verification of the RPH ("Emergency-Services-RPH-Validation-Passed", "Emergency-Services-RPH-Validation-Failed", and "No-Emergency-Services-RPH-Validation") have been defined but are subject to change based on decisions made by 3GPP. The means for signaling the "verstat" information associated with the RPH forwarded in the SIP INVITE message is for further study.

18. The ESRP interrogates the ECRF for routing instructions.
19. The ECRF returns the Route URI, i.e., the PSAP URI.
20. The ESRP forwards the INVITE to the egress BCF.
21. The egress BCF sends the INVITE to the PSAP.

[10] The HTTP interface used over the Ms interface needs to be enhanced to support the conveyance of the "rph" claim and associated assertion values.

[11] This call flow assumes that the incoming SIP INVITE contains a Resource-Priority header set to "esnet.1". If an incoming SIP INVITE message received by the BCF does not contain a Resource-Priority header, the BCF will add a Resource-Priority header set to "esnet.1" to the SIP INVITE message.

9.2 Call Flow for Emergency Callback Calls

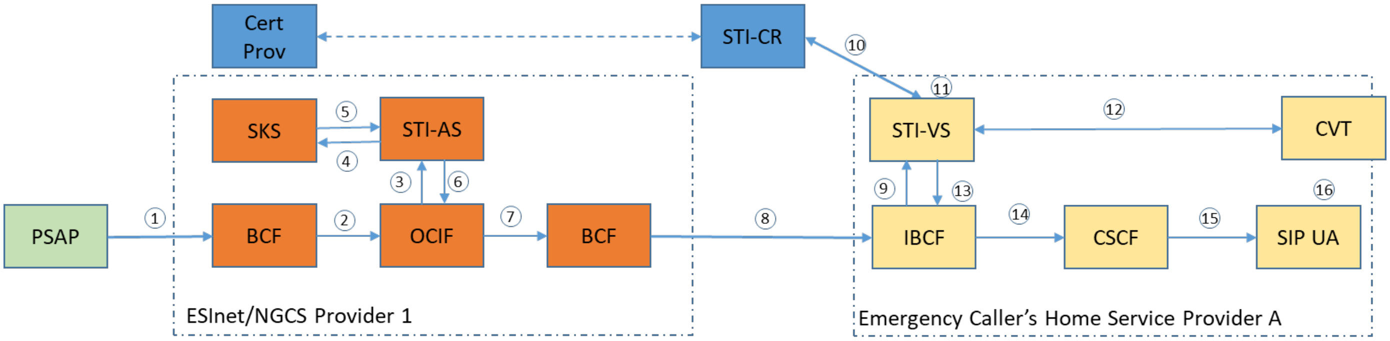

Figure 9.2: Emergency Services Callback Call Flow

1. The PSAP Call Handling Function initiates a callback with the callback number associated with the original emergency call in the To header and Request-URI, the TN of the PSAP originating the callback (i.e., sip:TN@<psapdomain>;user=phone) in the From and P-Asserted-Identity headers, "psap-callback" in the Priority header and the "esnet.0" in the Resource-Priority header, and forwards it to the BCF on the ingress side of the ESInet/NGCS.
2. The BCF forwards the INVITE to the OCIF.
3. The OCIF uses the destination address (i.e., the callback URI) in the Request-URI to determine the routing for the call. Before forwarding the call to an interconnecting IP network, the OCIF passes the SIP INVITE message to the STI-AS for authentication and signing of the Caller Identity and signing of the RPH and SIP Priority header.

   Note: The STI-AS must be invoked after originating call processing.

4. The STI-AS in the NGCS provider network first determines through service provider-specific means the legitimacy of the telephone number identity and RPH and SIP Priority header values being used in the INVITE. The STI-AS then securely requests its private key from the SKS.
5. The SKS provides the private key in the response, and the STI-AS signs the Caller Identity and the RPH/SIP Priority header and adds an Identity header field per ATIS-1000074-E [Ref 2] associated with the Caller Identity in the P-Asserted-Identity header field and an Identity header associated with the signed RPH/SIP Priority header.
6. The STI-AS passes the INVITE back to the NGCS OCIF.
7. If the BCF is not incorporated in the OCIF, the OCIF routes the call to the egress BCF.
8. The INVITE is routed over the NNI through the standard inter-domain routing configuration toward the emergency caller's home network via the entry IBCF in the interconnected network.
9. The emergency caller's home service provider (Service Provider A) entry IBCF initiates a verificationRequest in an HTTP POST message to the STI-VS that includes an identityHeader parameter associated with the Caller Identity and an identityHeader parameter associated with the RPH/SIP Priority header.

   Note: The STI-VS must be invoked before terminating call processing.

10. The home network SP STI-VS uses the "x5u" field in the PASSporT Protected Header per RFC 8225 [Ref 9] to determine the STI-CR Uniform Resource Identifier (URI) and makes an HTTPS request to the STI-CR.
11. The STI-VS validates the certificate (see Clause 5.3.1 of ATIS-1000074-E [Ref 2] for details) and then extracts the public key. It constructs the RFC 8224 [Ref 1] format and uses the public key to verify the signature in the Identity header fields, which validates the Caller Identity and RPH/SIP Priority header field content used when the Caller Identity and RPH/SIP Priority header content were signed by the STI-AS.
12. The STI-VS may interact with the CVT based on local policy and agreements between the emergency caller's home service provider and the CVT provider.
13. Depending on the result of the STI validation, the STI-VS returns a verificationResponse in an HTTP 200 OK message containing the verstatValue parameters (one associated with the Caller Identity and one associated with the RPH/SIP Priority header) to the IBCF.

Note: Provisional “verstat” values associated with verification of the RPH/SIP Priority header (“Emergency-Services-RPH-Priority-Header-Validation-Passed”, “Emergency-Services-RPH-Priority-Header-Validation-Failed”, or “No-Emergency-Services-RPH-Priority-Header-Validation), have been defined but are subject to change based on decisions made by 3GPP. The means for signaling the “verstat” information associated with the RPH/SIP Priority header forward in the SIP INVITE message, is for further study.

Note: Error cases where verification fails are discussed in Clause 5.3.2 of ATIS-1000074-E [Ref 2].

14. The IBCF continues to set up the call to the CSCF.
15. The CSCF continues to set up the call to the terminating SIP UA.
16. The terminating SIP UA receives the INVITE and normal SIP processing of the call continues, returning “200 OK” or optionally setting up media end-to-end.

10 Handling of Emergency Calls with Non-Dialable Callback Numbers

ATIS/TIA-J-STD-036-C-2, *Addendum to J-STD-036-C, Enhanced Wireless 9-1-1 Phase II* [Ref 19], Annex C, identifies a number of situations where a mobile station originating an emergency (9-1-1) call does not have a dialable callback number. In scenarios where a non-dialable callback number is appropriate, J-STD-036-C-2 specifies that the non-dialable callback number shall be of the form “911 + 7 least significant digits of the decimal representation of the Electronic Serial Number (ESN)” or “911 + last 7 digits of the International Mobile Equipment Identity (IMEI) expressed as decimal number”. ATIS-0700015 [Ref 3] and 3GPP TS 24.229 [Ref 8] describe procedures for processing 9-1-1 calls for which a dialable callback number is not available. In these scenarios, the SIP INVITE associated with the emergency origination will arrive at the E-CSCF with no P-Asserted-Identity header. The E-CSCF is then required to insert a P-Asserted-Identity header field set to a non-dialable callback number using one of the standard formats described above, before forwarding the SIP INVITE message to the LRF. If the LRF, based on interactions with the RDF, determines that the emergency call is destined for an NG9-1-1 Emergency Services Network, the emergency call will be routed by the E-CSCF to an exit IBCF in the originating IMS network with a non-dialable callback number included in the SIP INVITE message. Current procedures for applying Caller Identity authentication/RPH signing to 9-1-1 calls specify that, upon receiving a SIP INVITE associated with a 9-1-1 call, the IBCF will send signing requests to the STI-AS to request signing of the Caller Identity and RPH. The signing request associated with the Caller Identity information will typically include an ‘attest’ parameter indicating the attestation level associated with the Caller Identity. If the Caller Identity information consists of a non-dialable callback number that has been populated by the originating network E-CSCF, then the exit IBCF will send a signing request to the STI-AS with the non-dialable callback number populated in the “orig” parameter and a value of “A” populated in the “attest’ parameter. (The remaining parameters will be populated the same as for a 9-1-1 call with a dialable callback number.)

In addition, to ensure that the canonicalization process performed by the Authentication Service will not cause the content in the “orig” claim to be different than the content of the P-Asserted-Identity populated by the E-CSCF, which could cause the verification process to fail, clarifications were made to the Authentication Service and Verification Service, as described in ATIS-1000074-E [Ref 2] to address scenarios where an emergency call has a non-dialable callback number. Specifically, the Authentication Service procedures in ATIS-1000074-E [Ref 2] were modified to indicate that, if the calling TN identified in the P-Asserted-Identity (or From header field) is a non-dialable callback number formatted as defined in J-STD-036-C-2 [Ref 19], then the Authentication Service shall canonicalize the calling TN to remove any leading '+' sign or visual separators (e.g., internal dashes), and then populate the "orig" claim with the resulting digit string. Likewise, the Verification Service procedures were modified to indicate that if the calling TN identified in the P-Asserted-Identity or From header field associated with a 9-1-1 call is a non-dialable callback number formatted as described in J-STD-036-C-2 [Ref 19], then the Validation Service shall canonicalize the calling TN to remove any leading '+' sign or visual separators, and use the resulting digit-string to check the "orig" claim. The update to ATIS-1000074-E [Ref 2] notes that this special procedure shall be applied only if the non-dialable callback number is a digit-string of 10 digits with leading digits "911" or 11 digits with leading digits "1911".

11 Analysis

This clause describes the impacts on IMS Originating Networks and NG9-1-1 Emergency Services Networks of applying SHAKEN and RPH signing to 9-1-1 calls and SHAKEN, RPH signing and Priority header signing to callback calls. Open issues are also identified.

11.1Analysis of Impacts on IMS Originating Networks

The reference architectures and call flows to support the application of SHAKEN Caller Identity authentication and verification and RPH signing/verification to 9-1-1 calls, and the application of SHAKEN Caller Identity authentication and verification and RPH and SIP Priority header signing/verification to callback calls, as described in Clauses 8 and 9 of this document, highlight a number of impacts on existing functional elements within an IMS originating network and identify several new functional elements that must reside in or be accessible to IMS originating networks.

The P-CSCF may, based on local policy, be impacted by the application of SHAKEN and RPH signing mechanisms to 9-1-1 calls. This study identifies the following extensions to the P-CSCF functionality related to emergency call handling.

- A P-CSCF operating in an Originating Service Provider (OSP) network that supports calling number authentication and RPH signing may, based on local policy, be responsible for attesting to the identity of the calling user and inserting attestation information related to the asserted Caller Identity in an Attestation-Info header field within a SIP INVITE message associated with an emergency origination. The Attestation-Info header field will contain a value of "A", "B" or "C", as defined in ATIS-1000074-E [Ref 2].
- Based on local policy, if the P-CSCF is responsible for providing attestation information associated with the Caller Identity, the P-CSCF will insert a verstat parameter in P-Asserted-Identity header.
- When a node has performed attestation of an identity in an incoming request, it may also attest from where it received the request. It does so by sending a unique identifier identifying from where the request was received. Thus, a P-CSCF that performs attestation may also populate an optional origination identifier (in the form of a UUID) in an Origination-Id header field of a SIP INVITE message associated with an emergency origination. The value populated in the Origination-Id header field is based on local configuration and regulation.

Another originating network element that will be impacted by applying SHAKEN and RPH signing procedures to both 9-1-1 calls and callback calls is the IBCF. In support of caller authentication and RPH/Priority header signing related to 9-1-1 calls, the functionality and interfaces supported by an exit IBCF will be impacted in the following ways:

- Based on the reference architecture and call flow described in Clause 8.1 and 9, respectively, an exit IBCF in an IMS originating network that supports Caller Identity authentication and RPH signing will support an HTTP interface to an Authentication Service. It will send an HTTP POST message containing two signingRequests over the Ms reference point to the STI-AS. Based on local policy, the exit IBCF will populate the parameters in the signingRequests in one of two ways: either the IBCF will populate the information directly based on header fields received in the incoming SIP INVITE message (e.g., the Attestation-Info, Origination-Id), or it will need to derive the information to populate the claims in the signingRequests itself (e.g., based on other information in the SIP INVITE message or possibly via provisioning).
- Upon receiving an HTTP 200 OK message with signingResponses that include identityHeader parameters, the exit IBCF will use that information to populate Identity header fields (one associated with the signed Caller Identity and one associated with the signed RPH) in the outgoing SIP INVITE message.
- In addition, an exit IBCF in an IMS originating network that supports Caller Identity authentication and RPH signing will need to remove any verstat information that may be present in the P-Asserted-Identity or From header fields before forwarding the SIP INVITE message to the interconnecting NG9-1-1 Emergency Services Network. The exit IBCF may also, based on local policy, make a determination as to what information related to Caller Identity authentication and RPH signing should be forwarded to the interconnected Emergency Services Network based on the capabilities of that network.

In support of caller authentication and RPH verification related to callback calls, the functionality and interfaces supported by an entry IBCF in an emergency caller's home IMS network will be impacted in the following ways:

- If an entry IBCF in a SHAKEN-capable emergency caller's home network receives a SIP INVITE message that contains a 'verstat' populated as a tel uri parameter in the P-Asserted-Identity header field or From header field, the IBCF will remove the 'verstat' parameter from the message.
- If the emergency caller's home network has implemented the Ms reference point between the entry IBCF and the Verification Service to support verification of Caller Identity, RPH, and the SIP Priority header for callback calls, the entry IBCF will need to be capable of sending an HTTP verificationRequest and receiving a verificationResponse from the STI-VS . The entry IBCF will use the Identity header fields in the received SIP INVITE message to populate the identityHeader parameters in the HTTP verificationRequest.
- The entry IBCF will use verstatValue parameters received in the verificationResponse within an HTTP 200 OK message to populate 'verstat' information in the outgoing SIP INVITE message. The entry IBCF will populate the 'verstat' information associated with the Caller Identity as a tel uri parameter in the P-Asserted-Identity header field (or the From header field, if no P-Asserted-Identity header field is present). Further study is needed to determine how the 'verstat' associated with the RPH/SIP Priority header will be conveyed in the SIP INVITE message.

If the emergency caller's home network routes callback calls to an I/S-CSCF that is responsible for interacting with a Verification Service, then the I/S-CSCF will forward the SIP INVITE message associated with the callback call to the Verification Service prior to determining where to route the call. The I/S-CSCF will be responsible for receiving the SIP INVITE message back from the STI-VS with the 'verstat' information populated and using normal routing procedures to route the call to the emergency caller's UE.

In addition to the impacts on existing elements within an IMS Originating Network, support for Caller Identity authentication and RPH signing associated with 9-1-1 calls and Caller Identity, RPH, and SIP Priority header verification associated with callback calls will require that the originating network support (or provide access to) key elements in the SHAKEN framework architecture, including the STI-AS, STI-VS, SKS, STI-CR, and CVT. See Clause 8.1 for a description of these SHAKEN elements.

11.2 Analysis of Impacts on NENA i3 NG9-1-1 Emergency Services Networks

Consistent with the interconnection architecture described in ATIS-0700015 [Ref 3], the reference architectures and call flows described in Clauses 8 and 9, respectively, assume that the NG9-1-1 Emergency Services Network involved in routing the 9-1-1 calls and callback calls has been implemented using the NENA i3 architecture described in NENA-STA-010.3 [Ref 5]. To support Caller Identity authentication, RPH signing, and SIP Priority header signing for callback calls, and Caller Identity/RPH verification for 9-1-1 calls, the NENA i3 NG9-1-1 Emergency Services Network architecture will need to support interfaces to an Authentication Service (for callback calls) and a Verification Service (for 9-1-1 calls). In addition, there will be an impact to the way that 9-1-1 and callback calls are processed as a result of implementing SHAKEN Caller Identity authentication/verification and RPH signing/verification, and SIP Priority header signing mechanisms in NENA i3 ESInets/NGCS. Interactions between the Authentication Service/Verification Service and other SHAKEN functional elements (e.g., SKS, STI-CR, CVT) will also be needed to fully support Caller Identity authentication/verification and RPH signing/verification using the SHAKEN framework. The impacts on i3 NGCS related to support for SHAKEN Call Identity authentication/verification and RPH and SIP Priority header signing are summarized below.

- In addition to the functions typically provided by a BCF (e.g., admission control, firewall functionality), an entry BCF that receives a 9-1-1 call from an IMS originating network will need to determine whether an RPH set to "esnet.1" is present in the incoming SIP INVITE message. If the received SIP INVITE message does not include an RPH set to "esnet.1", the BCF will populate an RPH set to "esnet.1" in the SIP INVITE message. In addition, if a verstat parameter is present in the From or P-Asserted-Identity header field of the received SIP INVITE, the BCF must remove it prior to forwarding the SIP INVITE message to the ESRP.
- An ESRP that receives Identity headers in a SIP INVITE message associated with a 9-1-1 call will forward the SIP INVITE message to the STI-VS before determining where to route the call. Upon receiving the SIP INVITE message back from the STI-VS, the ESRP will perform location- and policy-based routing of the

9-1-1 call. The ESRP will pass the SIP INVITE message, including the Identity headers and verstat information, via a BCF to an i3 PSAP (or Legacy PSAP Gateway).[12]

- The OCIF, which plays a role in the handling of callback calls, will be responsible for interacting with the Authentication Service to request signing of the Caller Identity, RPH, and SIP Priority header, once it has determined that the call is destined for an interconnecting IP network. Specifically, the OCIF will pass the received SIP INVITE message to the STI-AS for authentication/signing of Caller Identity information, the RPH, and the SIP Priority header. Upon receiving the SIP INVITE message back from the STI-AS (with Identity headers associated with the signed Caller Identity and RPH/SIP Priority header), the OCIF will forward the SIP INVITE message via a BCF over the NNI toward the emergency caller's home network.

In addition to the impacts on existing elements within an i3 ESInet/NGCS, support for Caller Identity authentication and RPH/SIP Priority header signing associated with callback calls and Caller Identity and RPH verification associated with 9-1-1 calls will require that the i3 NG9-1-1 Emergency Services Network support (or provide access to) key elements in the SHAKEN framework architecture, including the STI-AS, STI-VS, SKS, STI-CR, and CVT. See Clause 8.1 for a description of these SHAKEN elements.

11.3 Open Issues

There are still open issues related to applying SHAKEN Caller Identity authentication/verification and RPH signing/verification to 9-1-1 calls and SHAKEN Caller Identity authentication/verification and RPH and SIP Priority header signing/verification to callback calls that may impact IMS originating networks.

One open issue is related to the handling of callback calls with private calling (PSAP) TNs. There are scenarios where a PSAP may want to keep their identity private when initiating a callback call (e.g., domestic violence scenarios). The ability to authenticate/verify the PSAP TN and convey the verification status associated with the Caller Identity to the called UE, even though the TN itself is not displayed to the called party, may improve the chances that a callback call gets answered. Currently, 3GPP standards only support conveyance of the 'verstat' as a parameter in a tel URI populated in a P-Asserted-Identity header or From header. However, consistent with IETF and 3GPP standards related to calling number privacy, a SIP INVITE associated with a callback call where the Caller Identity is to be kept private will omit the P-Asserted-Identity (which in the case of a callback call will contain the PSAP TN) and will contain a From header consisting of a sip URI of the form "sip:anonymous@anonymous.invalid". Since the P-Asserted-Identity header is not conveyed to the called UE, and the From header consists of a sip URI and not a tel URI, there is currently no standard way to communicate the 'verstat' to a called party if privacy of the calling number is invoked. One option for addressing this issue might be to convey the verstat in a parameter in the SIP URI. For callback calls with private calling numbers, this would result in a SIP INVITE being sent to the called UE that contains a From header formatted something like: sip:anonymous@anonymous.invalid;verstat=TN-Validation-Passed.

Public Safety is very concerned about caller location information being spoofed. They are seeking industry support for a mechanism, comparable to the signing/verification mechanism that has been specified for Caller Identity information, that would provide an indication of the trustworthiness of the location information associated with a 9-1-1 call. Thus, an additional open issue is related to defining a mechanism by which the trustworthiness of location information can be asserted/signed and verified. Considerations related to potential solutions that would allow for the "signing" and "verification" of location information need to address the fact the location may be delivered "by value" or "by reference". For example, there could be a scenario where the OSP is responsible for generating a location-by-value, as described in Clause 8.2.1 of ATIS-0700015 [Ref 3]. The OSP could extend the existing SHAKEN framework architecture to sign the Presence Information Data Format – Location Object (PIDF-LO), and the NG9-1-1 Emergency Services Network provider could use the existing framework for verification of that signed information. Another scenario to be considered is one where the signaling delivered to an originating network associated with an emergency (9-1-1) call contains a location-by-value, or where a UE provides location to a location server in the OSP network. The various ways in which location may be acquired suggest the potential need for something similar to the attestation levels defined for Caller Identity authentication. For example, an OSP that receives location-by-value from a UE could use a different "attestation" level to indicate that the location was generated by the UE rather than being generated by the OSP itself. Similarly, if the OSP receives location information in incoming signaling and performs some kind of consistency check on that information (e.g., checking

[12] If the next hop for the emergency call is another ESRP in the same ESInet, the subsequent ESRP will not repeat the verification process based on receipt of "verstat" information in the received SIP INVITE message.

whether the location information provided by the UE is consistent with location information obtained by location determination equipment in the OSP network), this might be indicated by associating a different “attestation” level with “sanity-checked” location information than would be associated with UE location that is just passed through by the OSP or location that is generated by the OSP. As noted above, location information may also be conveyed in the SIP INVITE “by reference”. Since location-by-reference is communicated in the Geolocation header within a SIP INVITE message, signing of location when sent “by-reference” would involve signing of the Geolocation header contents rather than the body (as would be the case when location-by-value is signed). While the conveyance of location-by-reference is viewed as reasonably secure, since it requires all entities that dereference the location to authenticate themselves, there might still be value, from the standpoint of spoofing mitigation, in having the OSP certify whether it populated the location-by-reference in the SIP INVITE message or some other entity did. The concept of signing location information, whether it be sent “by-value” or “by-reference”, requires further study.

As described in previous clauses within this document, there are still open issues related to the conveyance of ‘verstat’ information. As currently defined, ‘verstat’ can only be carried in a tel URI parameter used in the P-Asserted-Identity and the From header fields in a SIP request. 3GPP TS 24.229 [Ref 8] defines ‘verstat’ information only in the context of Caller Identity verification and only with the values “TN-Validation-Passed”, “TN-Validation-Failed”, and “No-TN-Validation”. While there is support within ATIS for separate ‘verstat’ values to be used to convey the verification results associated with a signed RPH or signed RPH/SIP Priority header, the final values will need to be adopted by 3GPP. In addition, a mechanism needs to be defined that will allow the ‘verstat’ associated with a verified RPH or RPH/SIP Priority header to be conveyed in a SIP INVITE message. As described above, considerations related to the signing of location information may require the definition of yet another set of ‘verstat’ values. This suggests the need for a general-purpose mechanism to support the communication of verification results associated with various types of information, with the appropriate protocol extensions made to HTTP and SIP to support the conveyance of verification results under various scenarios.

12 Potential Gaps in ATIS Standards Associated with the Application of SHAKEN Procedures to 9-1-1 and Callback Calls

This clause identifies gaps in the latest published versions of relevant ATIS specifications related to the application of SHAKEN procedures and RPH signing to 9-1-1 calls and SHAKEN, RPH signing and Priority header signing to callback calls.

12.1 ATIS-1000074-E

ATIS-1000074-E, *Errata on ATIS Standard on Signature-based Handling of Asserted information using toKENs [SHAKEN]* [Ref 15], published in 2019, does not specifically address the application of SHAKEN procedures to 9-1-1 calls or emergency callbacks. There has been ongoing work with the joint ATIS/SIP Forum IP-NNI Task Force to update ATIS-1000074-E [Ref 2] to include the necessary modifications to allow SHAKEN caller authentication and verification procedures to be applied to 9-1-1 calls and callback calls.

One change that was made was to allow the destination (i.e., “dest”) claim used in Caller Identity authentication and verification procedures to be of type “uri” if the “dest” claim contains a service URN in the ‘sos’ family. Previously, ATIS-1000074-E [Ref 2] limited the origination (i.e., “orig”) and “dest” claims to be in the form of a telephone number (i.e., of type “tn”). The expansion to allow “dest” claims of type “uri” was necessary because the Request-URI and possibly the To header in a SIP INVITE associated with a 9-1-1 call will contain an ‘sos’ service URN. In addition, further clarification was needed to the authentication and verification procedures to address a scenario where the Request-URI and the To header contain different information. This could be the case if the Request-URI contains a service URN in the ‘sos’ family, and the To header contains an emergency service number (e.g., the digits “911”, expressed as a URI). The draft update to ATIS-1000074-E [Ref 2] extends the SHAKEN procedures to specify that if the To header contains a telephone number that is an emergency service number, and the Request-URI contains an emergency service URN, the originating network may, based on local policy, update the To header to match the Request-URI prior to performing SHAKEN authentication. Furthermore, if the To header contains a telephone number that is an emergency service number and the Request-URI contains an emergency service URN, the SHAKEN verification procedures were clarified to state that normal SHAKEN verification should be performed.

In addition, the SHAKEN procedures defined in ATIS-1000074-E [Ref 2] specifically precluded calls with a SIP Resource-Priority Header (RPH) field from accessing Call Validation Treatment (CVT). This was done mainly with National Security / Emergency Preparedness Next Generation Network Priority Service (NS/EP NGN-PS) calls in mind, to ensure the highest probability of call completion for these types of calls. However, it was the view of Public Safety that 9-1-1 originations and callback calls could take advantage of analytics services provided by the CVT, so there was agreement in the joint ATIS/SIP Forum IP-NNI Task Force to update ATIS-1000074-E [Ref 2] to indicate that calls that contain a SIP RPH field may be passed to Call Validation Treatment, depending on the value of the namespace parameter in the RPH field and in accordance with local policy.

Most recently, updates were made to ATIS-1000074-E [Ref 2] to address the application of SHAKEN Caller Identity authentication procedures to 9-1-1 calls where the callback number is a non-dialable callback number. As described in Clause 10, if a dialable callback number cannot be associated with a 9-1-1 call for one of the reasons identified in Annex C of J-STD-036-C-2 [Ref 19] specifies that a non-dialable callback number derived from the ESN (i.e., “911” + “7 least significant digits of the decimal representation of the ESN”) or the IMEI (i.e., “911 + last 7 digits of IMEI expressed as decimal number”) shall be used to identify the emergency services caller. In these scenarios, the SIP INVITE associated with the emergency origination will arrive at the E-CSCF with no P-Asserted-Identity header. The E-CSCF inserts a P-Asserted-Identity header field set to a non-dialable callback number into the SIP INVITE prior to forwarding the message to LRF. If the LRF, based on interactions with the RDF, determines that the emergency call is destined for an NG9-1-1 Emergency Services Network, the emergency call will be routed by the E-CSCF to an exit IBCF in the originating network with a non-dialable callback number included in the SIP signaling. Updates to ATIS-1000074-E [Ref 2] specify that, upon receiving a SIP INVITE associated with a 9-1-1 call where the Caller Identity is a non-dialable callback number formatted as described in ATIS/TIA-J-STD-036-C-2 [Ref 19], the IBCF will send a signing request to the STI-AS to request signing of the Caller Identity, and that signing request will include an ‘attest’ parameter with the value “A”.

12.2 ATIS-0700015

ATIS-0700015 [Ref 3], *ATIS Standard for Implementation of 3GPP Common IMS Emergency Procedures for IMS Origination and ESInet/Legacy Selective Router Termination*, focuses on architectures and procedures to support emergency communications originating from IMS subscribers and delivered to i3 ESInets or legacy Selective Routers. These architectures and procedures do not currently support Caller Identity authentication/verification or RPH signing/verification associated with emergency originations or Caller Identity authentication/verification or RPH/SIP Priority header signing/verification associated with callback calls.

To support Caller Identity authentication/verification and RPH and SIP Priority header signing/verification based on the SHAKEN framework, the architecture illustrated in Figure 7-2 of ATIS-0700015 [Ref 3] will need to be further expanded to describe the interaction between the IMS originating network elements and the SHAKEN architecture elements. In the case of emergency (9-1-1) originations, this will mean incorporating the Ms reference point into the ATIS-0700015 [Ref 3] architecture to allow interactions between the exit IBCF and the SHAKEN Authentication Service (i.e., STI-AS) to support the authentication/signing of Caller Identity and RPH information. The interaction between emergency call processing and SHAKEN may also require updates to the procedures defined in ATIS-1000015[Ref 3] associated with existing elements, such as the P-CSCF and the IBCF. Updates may also be needed to the assumptions and requirements associated with the interconnection of IMS originating networks and i3 ESInets. Since work on defining call authentication in non-IP networks is just beginning, further study is needed to determine what impacts, if any, there will be on assumptions, requirements and procedures specified in ATIS-0700015 [Ref 3] related to the interconnection of IMS originating networks with legacy SRs.

The material in ATIS-0700015 [Ref 3] related to callback calls is currently very limited and consists of a single statement indicating that callback calls to a UE that originated an emergency call are treated like any other call to that UE. Since the signaling associated with emergency calls that are routed via an i3 ESInet will include a marking specifically identifying the call as a “psap-callback”, and there is an expectation that Caller Identity and RPH/SIP Priority header verification will be performed by the emergency caller’s home network on callback calls, consideration should be given to extending ATIS-0700015 [Ref 3] to allow UEs to apply special processing to callback calls, based on local policy, and to support an interface from an IMS core element in the emergency caller’s home network to the SHAKEN Verification Service (i.e., STI-VS) to support the verification of Caller Identity and RPH/SIP Priority header information associated with the callback call.

Procedures related to the application of SHAKEN to emergency calls with non-dialable callback numbers will also impact ATIS-0700015 [Ref 3]. In addition, Public Safety is very concerned about caller location information being spoofed. They are seeking industry support for a mechanism, comparable to the signing/verification mechanism that has been specified for Caller Identity information, that would provide an indication of the trustworthiness of the location information associated with a 9-1-1 call. The concept of signing location information, whether it be sent “by-value” or “by-reference” requires further study but could potentially impact ATIS-0700015 [Ref 3].

12.3 ATIS-0500032

ATIS-0500032, *ATIS Standard for Implementation of an IMS-based NG9-1-1 Service Architecture* [Ref 16], describes an IMS-based NG9-1-1 Service Architecture. The current published version of this document does not address Caller Identity authentication/verification or RPH or SIP Priority header signing/verification. Work is underway within ATIS to update this document to identify the impacts on IMS-based NG9-1-1 Emergency Services Networks of applying SHAKEN and RPH signing to 9-1-1 originations and SHAKEN, RPH and SIP Priority header signing to callback calls. As part of this effort, the IMS-based NG9-1-1 Emergency Services Network architecture will need to be extended to include an Ms reference point between an entry IBCF and a Verification Service (i.e., STI-VS) to support the verification of Identity headers associated with Caller Identity and RPH information received in SIP INVITE messages related to emergency originations. To support Caller Identity and RPH/SIP Priority header signing/verification in the context of callback calls, the architecture described in ATIS-0500032 will also need to support a SIP interface between a Transit Function and an Authentication Service (i.e., STI-AS). Alternatively, an Ms reference point between an exit IBCF and an STI-AS may be used to support Caller Identity authentication and RPH/SIP Priority header signing for callback calls.

There are currently several call flows in ATIS-0500032 that illustrate different 9-1-1 scenarios (e.g., 9-1-1 calls originating in legacy, IMS, and non-IMS IP networks, and terminating at legacy and i3 PSAPs with location-by-reference or location-by-value). Modifications and additions will need to be made to the existing set of call flows to illustrate the application of SHAKEN Caller Identity authentication/verification and RPH signing/verification to 9-1-1 calls and SHAKEN Caller Identity authentication/verification and RPH/SIP Priority header signing/verification to callback calls. Public Safety representatives have expressed a desire to receive attestation information as well as verification status associated with Caller Identity information with a 9-1-1 call. ATIS-0500032 will need to be updated to address the ability for an IMS-based NG9-1-1 Emergency Services Network to convey attestation level and verification status information to an i3 PSAP. There is still an open issue regarding a mechanism for conveying RPH verification status information in SIP signaling. In addition, ATIS-0500032 will need to consider how SHAKEN-related information, like attestation level and verification status, can be passed between PSAPs when transferring a call on an intranetwork basis. The SIP INVITE header profile will also need to be updated to address conveyance of Identity headers containing signed Caller Identity and RPH information.

12.4 ATIS-0500036

ATIS-0500036, *ATIS Standard for IMS-based Next Generation Emergency Services Network Interconnection* [Ref 17], addresses the interconnection of IMS-based NG9-1-1 Emergency Services Networks with other legacy and NG9-1-1 (i.e., IMS-based and i3) Emergency Services Networks to support the delivery of initial and transferred emergency calls. It is anticipated that future work on this document will be needed to describe what happens to signed Caller Identity and RPH information (and associated attestation and verification status information) when an emergency call is transferred between Emergency Services Networks. In addition, consideration needs to be given to if/when it is appropriate to repeat the authentication/signing process (e.g., associated with the RPH header field content) in the upstream NG9-1-1 Emergency Services Network, and to repeat the verification process in the downstream NG9-1-1 Emergency Services Network.

13 Conclusion

This Technical Report analyzes the impacts on IMS originating networks of applying STIR/SHAKEN Caller Identity authentication and verification, and RPH and SIP Priority header signing/verification to 9-1-1 calls and callback calls, with a focus on identifying potential impacts to ATIS-0700015 [Ref 3]. It describes the potential value of applying SHAKEN Caller Identity authentication and RPH/SIP Priority header signing/verification to address threat scenarios in a Public Safety environment. High-level architecture and call flow descriptions were also provided to illustrate the impacts on originating networks and NENA i3 ESInets/NGCS associated with applying SHAKEN and RPH/Priority header signing/verification to 9-1-1 calls and callback calls. This study further summarizes other relevant ATIS and 3GPP standards and the extensions that would be needed to those documents to address

SHAKEN Caller Identity authentication and verification in a 9-1-1 environment and to support RPH and Priority header signing and verification in the context of 9-1-1 calls and callback calls.

This study summarizes the impacts on IMS originating networks and NENA i3 ESInets/NGCS of supporting Caller Identity authentication/verification and RPH and Priority header signing/verification for 9-1-1 calls and callback calls and identifies open issues that still need to be addressed. Finally, Clause 14 of this Technical Report provides recommendations regarding updates to ATIS-0700015 [Ref 3].

14 Recommendations

This clause contains recommendations regarding the update of ATIS-0700015 [Ref 3] to address SHAKEN for 9-1-1 calls and callback calls.

- The Assumptions and Requirements currently documented in ATIS-0700015 [Ref 3] should be updated to capture the applicable assumptions documented in this Technical Report. Requirements related to the P-CSCF should be updated to specify that a P-CSCF may, based on local policy, associate an RPH in the 'esnet' namespace with an emergency origination. In addition, a P-CSCF may also insert a verstat parameter in the P-Asserted-Identity header, and optional Attestation-Info and Origination-Id header fields in the SIP INVITE message associated with an emergency origination. This information may be used by downstream Caller Identity authentication and verification processes.

  Updated material should also capture additional requirements associated with an exit IBCF applicable to its role in the Caller Identity and RPH authentication/signing process. These would address interactions that the IBCF has with the Authentication Service and additional procedures related to preparing the SIP INVITE message associated with an emergency origination for delivery to an i3 ESInet/NGCS.

  Requirements applicable to an entry IBCF that is receiving a callback call may also need to be specified. Based on local policy, an entry IBCF may be responsible for interacting with a Verification Service. This capability should be captured in the update to ATIS-0700015 [Ref 3].

- Updates will be needed to the architecture currently described in ATIS-0700015 [Ref 3] to include the SHAKEN elements relevant to Caller Identity authentication/verification and RPH signing/verification, and their relationship to the IMS Functional Elements described in Clause 7. Consideration will need to be given to how best to illustrate the extensions to the existing architecture (i.e., whether existing diagrams should be updated or a new diagram added). Descriptions of the SHAKEN elements should be included in the update to ATIS-0700015 [Ref 3], with appropriate references to ATIS-1000074-E [Ref 2]. The material in Clause 7.6, *Procedures Related to Establishment of IMS Emergency Session*, may be expanded to describe the application of SHAKEN Caller Identity authentication and RPH signing to the establishment of an emergency session.

- Updates to the Stage 3 material currently in Clause 8 of ATIS-0700015 [Ref 3] will be needed to include a definition for the Ms reference point and call flows that illustrate the application of SHAKEN Caller Identity authentication/verification and RPH signing/verification to emergency originations. Consideration should be given to expanding the material in ATIS-0700015 [Ref 3] related to callback calls to describe unique signaling characteristics of callback calls routed via an i3 ESInet and the impacts on an IMS home network of applying Caller Identity and RPH/SIP Priority header verification procedures to such calls. The addition of one or more diagrams illustrating a callback call flow may be desirable. In addition, the content addressing procedures at the P-CSCF and IBCF should be expanded to address functionality associated with applying SHAKEN Caller Identity authentication/verification and RPH signing/verification to 9-1-1 calls and SHAKEN Caller Identity authentication/verification and RPH/SIP Priority header signing/verification to callback calls.

- The *SIP INVITE Profile for Emergency Calls* provided in Annex A should be updated to address the conveyance of Identity headers in a SIP INVITE associated with an emergency call.

- Consideration should also be given to updating the Message Examples provided in Annex E to illustrate the inclusion of Identity header fields, and other SHAKEN-related information (e.g., 'verstat', Attestation-Info, Origination-Id) in SIP signaling messages and the exchange of application messages to support signing and verification of Caller Identity and RPH content.