ATIS-0500044

Overview and Operational Considerations Related to the Application of Information Spoofing Mitigation Techniques to 9-1-1 and Callback Calls in an End-State NG9-1-1 Environment

TECHNICAL REPORT

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

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

ATIS-0500044, *Overview and Operational Considerations Related to the Application of Information Spoofing Mitigation Techniques to 9-1-1 and Callback Calls in an End-State NG9-1-1 Environment*

Published by

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

ATIS-0500044

ATIS Technical Report on

Overview and Operational Considerations Related to the Application of Information Spoofing Mitigation Techniques to 9-1-1 and Callback Calls in an End-State NG9-1-1 Environment

Alliance for Telecommunications Industry Solutions

Approved August 16, 2021

Abstract

This Technical Report provides an overview and addresses operational considerations related to the application of information spoofing mitigation mechanisms, like Signature-based Handling of Asserted Information Using toKENs (SHAKEN), to 9-1-1 calls and callback calls in an end-state NG9-1-1 environment.

Foreword

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

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

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

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

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

R. Muscat, ESIF Chair (Bexar Metro 911)

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

J. Torres, ESIF 2nd Vice Chair (Verizon Wireless)

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

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

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

Table of Contents

Table of Figures

ATIS Technical Report on –

Overview and Operational Considerations Related to the Application of Information Spoofing Mitigation Techniques to 9-1-1 and Callback Calls in an End-State NG9-1-1 Environment

1 Scope, Purpose, & Application

1.1 Scope

There is a strong emphasis being placed by regulators in North America on strategies for combatting nuisance calls, including robocalls and calls where the caller identity is illegitimately spoofed. Caller authentication techniques, such as those described in ATIS standards related to Signature-based Handling of Asserted Information Using toKENs (SHAKEN) and Internet Engineering Task Force (IETF) RFCs related to Secure Telephone Identity Revisited (STIR), have been developed to allow calls traveling through interconnected carrier networks to have the legitimacy of the caller's identity evaluated by the originating carrier and validated by the terminating carrier, facilitating the delivery of an indication of the legitimacy of the caller identity information to the called party. Work is underway within ATIS to address the application of SHAKEN to 9-1-1 calls and callback calls, and to define techniques for mitigating the spoofing of other call-related information, such as Session Initiation Protocol (SIP) Resource-Priority header fields and Priority header fields.

This Technical Report provides a high-level description of the impacts on the processing of 9-1-1 calls and callback calls associated with the application of information spoofing mitigation techniques in an end-state Next Generation 9-1-1 (NG9-1-1) environment. The Technical Report also includes a roadmap describing the various standards/specifications that address this topic, and highlights the operational impacts associated with the application of false data manipulation mitigation techniques to 9-1-1 and callback call processing.

1.2 Purpose

This Technical Report provides an overview and analysis of operational impacts associated with applying STIR/SHAKEN caller identity authentication/verification and Resource-Priority Header (RPH) and Priority header signing/verification to 9-1-1 calls and callback calls.

1.3 Application

This Technical Report applies to emergency (9-1-1) calls originated in IP Multimedia Subsystem (IMS) networks in North America and delivered via NG9-1-1 Emergency Services Networks to i3 Public Safety Answering Points (PSAPs) to assist in the detection and mitigation of spoofed call/caller information. This Technical Report also applies to callback calls originated by i3 PSAPs and delivered via NG9-1-1 Emergency Services Networks to IMS networks that serve emergency callers to mitigate false data manipulation associated with callback calls. 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 1], and ATIS-1000098, *Session Initiation Protocol (SIP) Resource-Priority Header (RPH) and Priority Header Signing in Support of Emergency Calling* [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 su98 of applying the most recent editions of the standards indicated below.

[Ref 1] ATIS-1000074-E, *Errata on ATIS Standard on Signature-based Handling of Asserted information using toKENs (SHAKEN)*.[1]

[Ref 2] ATIS-1000098, *Session Initiation Protocol (SIP) Resource-Priority Header (RPH) and Priority Header Signing in Support of Emergency Calling*.[1]

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

[Ref 3] IETF RFC 8224, *Authenticated Identity Management in the Session Initiation Protocol (SIP)*.[2]
[Ref 4] IETF RFC 8225, *PASSporT: Personal Assertion Token*.[2]
[Ref 5] IETF RFC 7090, *Public Safety Answering Point (PSAP) Callback*. [2]
[Ref 6] IETF draft-ietf-stir-rph-emergency-services, *Assertion Values for a Resource Priority Header Claim and a SIP Priority Header Claim in Support of Emergency Services Networks*. [2]
[Ref 7] ATIS-1000080, *Signature-based Handling of Asserted information using toKENs (SHAKEN): Governance Model and Certificate Management.* [1]
[Ref 8] ATIS-1000081, *ATIS Technical Report on a Framework for Display of Verified Caller ID.*
[Ref 9] ATIS-1000082, *Technical Report on SHAKEN APIs for a Centralized Signing and Signature Validation Server*. [1]
[Ref 10] ATIS-1000084, *Technical Report on Operational and Management Considerations for SHAKEN STI Certification Authorities and Policy Administrators*. [1]
[Ref 11] RFC 8443, *Personal Assertion Token (PASSporT) Extension for Resource Priority Authorization*. [2]
[Ref 12] ATIS-0500032, *ATIS Standard for Implementation of an IMS-based NG9 1 1 Service Architecture*. [1]
[Ref 13] ATIS-0500036, *ATIS Standard for IMS-based Next Generation Emergency Services Network Interconnection*. [1]
[Ref 14] ATIS-0700015, *ATIS Standard for Implementation of 3GPP Common IMS Emergency Procedures for IMS Origination and ESInet/Legacy Selective Router Termination*. [1]
[Ref 15] ATIS-0700048, *Study of SHAKEN Impacts on 9-1-1 Calls and Callback Calls*. [1]
[Ref 16] IETF RFC 8558, *Personal Assertion Token (PASSporT) Extension for Signature-based Handling of Asserted information using toKENs (SHAKEN).* [2]
[Ref 17] 3GPP TS 23.167, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; *IP Multimedia Subsystem (IMS) emergency sessions*.[3]
[Ref 18] 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*.[3]
[Ref 19] ATIS/TIA J-STD-036-C-2, Enhanced Wireless 9-1-1 Phase II. [1]
[Ref 20] FCC Report and Order and Further Notice of Proposed Rulemaking In the Matter of Call Authentication Trust Anchor and Implementation of TRACED Act Section 6(a) —Knowledge of Customers by Entities with Access to Numbering Resources.[4]
[Ref 21] Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act.[5]

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

Callback Call: A request whose purpose is to re-contact the party that originated an emergency call.

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

Emergency Call: A generic term used to include any type of Request For Emergency Assistance (RFEA). In North America, the 3-digit code “911” is typically used to facilitate the reporting of an emergency requiring response by a Public Safety agency.

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.

---

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

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

[4] This document is available from the FCC at: < https://docs.fcc.gov/public/attachments/FCC-20-42A1_Rcd.pdf >.

[5] This document is available at: < https://www.congress.gov/bill/116th-congress/senate-bill/151/text >.

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 5] for further details.

3.2 Acronyms & Abbreviations

3GPP	Third Generation Partnership Project
API	Applications Programming Interface
ATIS	Alliance for Telecommunications Industry Solutions
BCF	Border Control Function
CA	Certification Authority
CDR	Call Detail Record
CN	Core Network
CPE	Customer Premises Equipment
CSCF	Call Session Control Function
CVT	Call Validation Treatment
ECRF	Emergency Call Routing Function
E-CSCF	Emergency Call Session Control Function
ESInet	Emergency Services IP network
ESN	Electronic Serial Number
ESRP	Emergency Service Routing Proxy
FCC	Federal Communications Commission
FNPRM	Further Notice of Proposed Rulemaking
HTTP	Hyper Text Transfer Protocol
IBCF	Interconnection Border Control Function
I-CSCF	Interrogating Call Session Control Function
ID	Identification
IETF	Internet Engineering Task Force
IM	IP Multimedia
IMEI	International Mobile Equipment Identity
IMS	IP Multimedia Subsystem
IP	Internet Protocol
LRF	Location Retrieval Function
LS	Location Server
NENA	National Emergency Number Association
NG9-1-1	Next Generation 9-1-1
NGCS	Next Generation Core Service
NNI	Network-to-Network Interface
OCIF	Outbound Call Interface Function
PASSporT	Personal Assertion Token
PCA	PSAP Credentialing Agency
P-CSCF	Proxy Call Session Control Function
PKI	Public Key Infrastructure
PSAP	Public Safety Answering Point

PSTN	Public Switched Telephone Network
RDF	Routing Determination Function
REST	Representational State Transfer
RFEA	Request For Emergency Assistance
RPH	Resource-Priority Header
RTT	Real Time Text
SDP	Session Description Protocol
SHAKEN	Signature-based Handling of Asserted information using toKENs
SIP	Session Initiation Protocol
SKS	Secure Key Store
SOP	Standard Operating Procedure
STI	Secure Telephone Identity
STI-AS	Secure Telephone Identity Authentication Service
STI-CA	Secure Telephone Identity Certification Authority
STI-CR	Secure Telephone Identity Certificate Repository
STI-PA	Secure Telephone Identity Policy Administrator
STIR	Secure Telephone Identity Revisited
STI-VS	Secure Telephone Identity Verification Service
TN	Telephone Number
TRACED	Telephone Robocall Abuse Criminal Enforcement and Deterrence
UE	User Equipment
URI	Uniform Resource Identifier
URN	Uniform Resource Name
VoIP	Voice over Internet Protocol

4 Background

SHAKEN is being used in telecom networks to combat robocalling and caller identity spoofing. There is value in extending the SHAKEN capability to address spoofing mitigation for 9-1-1 calls and callback calls. Voice over Internet Protocol (VoIP) Service Providers are currently deploying spoofing mitigation solutions based on the SHAKEN procedures defined by ATIS and the Secure Telephone Identity (STI) protocols defined by IETF. Recent industry activity has focused on defining the interactions between the SHAKEN caller identity authentication/verification mechanisms and the processing of 9-1-1 calls and callback calls. In addition, mechanisms have been defined to support the signing of other call-related information, such as the information communicated in the RPH field, to prevent the misuse of resources associated with 9-1-1 and callback calls.

The SHAKEN framework, described in ATIS-1000074-E [Ref 1], assumes that the originating voice service provider attests to the caller's identity, and the terminating voice service provider verifies the identity of the originator of the message that contains the caller identity. The SHAKEN framework defines three levels of attestation which reflect the ability of the originating network provider to vouch for the accuracy of the source of origin of the call. For example, if the originating service provider has an authenticated direct relationship with the originator of the call, this attestation is categorized differently than calls that are originated from different networks or gateways. As specified in ATIS-1000074-E [Ref 1], these attestation levels are defined as follows:

A. Full Attestation, where the signing provider:

- Is responsible for the origination of the call
- Has direct relationship with and can identify the customer
- Has established a verified association with the telephone number used for the call

B. Partial Attestation, where the signing provider

- Is responsible for the origination of the call
- Has a direct relationship with the customer and can identify the customer
- Has not established a verified association with the telephone number being used for the call

C. Gateway Attestation, where the signing provider

- Is the entry point of the call into its VoIP network
- Has no relationship with the initiator of the call (e.g., call is entering from an international gateway)
- Is not asserting anything other than the fact that this is the point where the call entered its network

An attestation level of "A" indicates that the signing provider is attesting to the fact that the call has been originated by their customer, and that their customer can "legitimately" use the number that appears as the caller identity. An "A" attestation may also be used to convey that the signing service provider has determined (e.g., by business agreement) that the customer is authorized to use a number, even if the number was assigned by another service provider. An "A" attestation may also be associated with a number that is not permanently assigned to an individual customer, but that can be tracked by the signing provider as being used by a customer for certain calls or during a certain timeframe. Ultimately, it is up to service provider policy to decide what constitutes a "legitimate right to assert a telephone number". In populating an attestation level of "B", the service provider attests that it can trace the source of the call to a customer for policy enforcement purposes. By asserting an attestation level of "C", the signer/originating service provider indicates that it should be able to trace a call to an interconnecting service provider and/or peer node for traceback or policy enforcement purposes. Although an attestation level of "C" is referred to as "Gateway Attestation", it may also be used when there is not sufficient information to apply an "A" or "B" attestation, even when the call was received at a customer interface.

The SHAKEN architecture calls for the originating service provider to use X.509-based certificates to "sign" the call information. The certificate indicates that the signer of the call information is who it claims to be, that it is authorized to sign for the number originating the call, and that its claims about the call it is authenticating can be trusted. The terminating service provider then verifies that signature which helps it to determine the level of trust in the call information provided by the originating service provider. It is important to note that the verification process confirms the identity of the signer of the received content, but it does not specifically verify the caller identity itself.

Because the SHAKEN framework relies on transmission of information via Session Initiation Protocol (SIP) messages, it can only operate on the Internet Protocol (IP) portions of a voice service provider's network, i.e., those portions served by network technology that is able to initiate, maintain, and terminate SIP calls. If a call terminates on a network or is routed at any point over an intermediate provider network that does not support the transmission of SIP calls, the SHAKEN-related information will be lost.

In the Report and Order and Further Notice of Proposed Rulemaking [Ref 20], adopted and released on March 31, 2020, by the Federal Communications Commission (FCC) in response to the Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act [Ref 21], an implementation deadline of June 30, 2021, is set for voice service providers to implement the SHAKEN caller identity authentication framework in the IP portions of their networks. Specifically, the Report and Order requires that:

(i) a voice service provider that originates a call that exclusively transits its own network must authenticate and verify the caller ID information consistent with the STIR/SHAKEN authentication framework;

(ii) a voice service provider originating a call that it will exchange with another voice service provider or intermediate provider must authenticate the caller ID information in accordance with the STIR/SHAKEN authentication framework and, to the extent technically feasible, transmit that caller ID information with authentication to the next provider in the call path; and

(iii) a voice service provider terminating a call with authenticated caller ID information it receives from another provider must verify that caller ID information in accordance with the STIR/SHAKEN authentication framework.

The TRACED Act [Ref 21] contains a provision that requires voice service providers to take "reasonable measures" to implement an effective caller identity authentication framework in the non-IP portions of their networks. In their Further Notice of Proposed Rulemaking (FNPRM), the FCC interprets that provision as being satisfied only if a

voice service provider is actively working to implement a caller ID authentication framework on the non-IP portions of its network, either by upgrading its non-IP networks to IP so that the SHAKEN authentication framework may be implemented, or by working to develop a non-IP authentication solution. Industry activities are underway that are focused on identifying alternative mechanisms for supporting caller authentication for non-IP traffic.

While the FCC Report and Order [Ref 20] makes specific references to “voice service providers”, the TRACED Act [Ref 21] also seeks to protect subscribers from receiving unwanted text messages as well as voice calls from callers that use an unauthenticated number. At this time, the SHAKEN framework defined in ATIS-1000074-E [Ref 1] does not specifically apply to Short Message Service (SMS) text to 9-1-1 messages and MMS text to 9-1-1 messages; however, the existing architectures, procedures, and protocols defined in ATIS-1000074-E [Ref 1] and ATIS-1000098 [Ref 2] could potentially be used to support caller identity authentication for Real Time Text (RTT) originations to 9-1-1.

The FCC and the industry recognize that SHAKEN is not a “silver bullet” in the fight against caller identity spoofing, but it is an important tool in the illegal spoofing mitigation toolbox. It is important that the landscape remain flexible in identifying and testing new techniques to continually adapt to the evolving ploys of bad actors who intend to defraud or cause harm to public safety.

5 Assumptions

The following are assumptions regarding the application of information spoofing mitigation techniques to 9-1-1 calls and callback calls that apply in the context of this Technical Report.

1. An RPH in the ‘esnet’ namespace may or may not be associated with an emergency origination by the originating IMS network, based on local policy.
2. 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 an NG9-1-1 Emergency Services Network.
3. The NG9-1-1 Emergency Services Network will be responsible for performing verification of the signed caller identity/RPH information received with an emergency call.
4. Callback calls routed via the NG9-1-1 Emergency Services Network will be marked as “psap-callback” and will contain an RPH with a value of “esnet.0”.
5. The NG9-1-1 Emergency Services Network will be responsible for performing caller identity attestation/authentication and RPH and Priority header signing on callback calls.
6. Verification of a signed caller identity/RPH/Priority header will be performed by the emergency caller’s home network for a callback call if SHAKEN/RPH/Priority header verification is supported by that network.
7. A Service Provider can use the same certificates for signing SIP RPH and Priority headers as they use for telephone number (TN) signing but is not required to do so.
8. SIP RPH signing does not change or modify 9-1-1/callback call processing, signaling, and routing procedures (although it may result in additional information being included in the signaling associated with the 9-1-1 call or callback call); it simply provides a security tool for transit and receiving providers to determine if the SIP RPH is trusted.
9. If validation 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, as well as the results of the caller identity and RPH verification.
10. A separate indicator will be used to convey RPH signing verification success/failure.
11. If validation of the signed caller identity, SIP RPH or Priority header associated with a callback call fails, the local policy of the emergency caller’s home network provider will determine terminating call processing, such as whether the call should be delivered with caller identity and/or SIP RPH/Priority header information intact. Note that if the call proceeds, separate verification status parameters will be included in the associated SIP signaling to reflect the verification status of the caller identity and the verification status of the SIP RPH/Priority header.
12. For emergency originations, signing of caller identity is separate from SIP RPH signing. Separate SIP Identity headers are used for SIP RPH signing and caller identity signing.

13. For callback calls, SIP RPH signing is coupled with Priority header signing, and is separate from caller identity authentication. A single Identity header is associated with the signed RPH/Priority header, and a separate Identity header is associated with the signed caller identity.
14. Callback calls will use normal routing (i.e., via the emergency caller's home network) to the network that is serving the emergency caller.
15. Verstat information associated with the callback call will be delivered to the emergency caller's User Equipment (UE).
16. Caller identity attestation and verification status (i.e., verstat) information associated with a 9-1-1 call will be delivered to the i3 PSAP Call Handling functional element and will be displayed to the i3 PSAP call taker.
17. RPH verification status associated with a 9-1-1 call will be delivered to the i3 PSAP Call Handling functional element but will not be displayed to the i3 PSAP call taker.

6 Use Cases

This section describes use cases associated with the application of caller identity authentication/verification and RPH signing/verification to 9-1-1 calls and callback calls, and SIP Priority header signing/verification to callback calls.

6.1 Use Case #1: 9-1-1 Call Origination with Authentication/Signing and Verification of Dialable Callback Number and Resource-Priority Header Performed

Short Description

A caller places a 9-1-1 call and the caller's identity undergoes attestation/authentication in the originating network, the RPH field is signed in the originating network, and both caller identity and RPH undergo verification in the NG9-1-1 Emergency Services Network. The 9-1-1 call is then delivered to an i3 PSAP.

Actors

Bob is the caller whose UE originated the emergency call.

Carol is the PSAP call taker at an i3 PSAP to which the emergency call is delivered.

Pre-Conditions

Bob originates a 9-1-1 call from UE that has a dialable callback number associated with it.

Post-Conditions

Carol is in communication with Bob and is handling his 9-1-1 call.

Normal Flow – Originating network associates an Attestation Level of "A" with the caller identity; caller identity and RPH are successfully signed and verified

1. Bob initiates an emergency call, and the call request is forwarded to the originating network.
2. The origination network associates a dialable callback number, an appropriate RPH value, and location information with the call.
3. The originating network associates an attestation level of "A" with the caller identity (i.e., callback number). [Note: Attestation may happen either before or after call routing.]

4. The originating network performs location-based routing (may not be the caller's location) of the 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 are signed.
6. The originating network routes the 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 that performs verification of the signed caller identity and RPH. In this use case, the verification is successful.
8. The NG9-1-1 Emergency Services Network applies location- and policy-based routing to the 9-1-1 call.
9. The NG9-1-1 Emergency Services Network delivers the 9-1-1 call to the i3 PSAP with callback information (and associated verification status and attestation level), RPH (and associated verification status), and location (by-value or by-reference).
10. Carol answers the call.
11. In parallel, Carol'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.
12. Bob's location information and callback information are displayed on Carol's Customer Premises Equipment (CPE), along with the verification status and attestation level associated with the callback number.
13. Carol handles the call according to Operating Procedures applicable to a 9-1-1 call where the caller identity has an attestation level of "A" and is signed and verified.

Alternate Flow #1 – Originating network associates an Attestation Level of "C" with the caller identity; caller identity and RPH are successfully signed and verified

3. The originating network associates an attestation level of "C" with the caller identity (i.e., callback number). [Note: Attestation may happen either before or after call routing.]
13. Carol handles the call according to Operating Procedures applicable to a 9-1-1 call where the caller identity is has an attestation level of "C" and is signed and verified. Handling of this call may be the same as a pre-SHAKEN call (where attestation and verification status information are not available).

Alternate Flow #2 – Originating network associates an Attestation Level of "A" with the caller identity; caller identity and RPH are signed but verification fails

7. The NG9-1-1 Emergency Services Network interacts with a Verification Service that performs verification of the signed caller identity and RPH. In this use case, the verification fails.
13. Carol handles the call according to Operating Procedures applicable to a 9-1-1 call where the caller identity is has an attestation level of "A" but verification has failed. Handling of this call may be the same as a pre-SHAKEN call (where attestation and verification status information are not available).

6.2 Use Case #2: Emergency Callback with Authentication and Verification of i3 PSAP Calling Number, Resource-Priority Header, and SIP Priority Header Performed

Short Description

An i3 PSAP places an emergency callback call (e.g., because the emergency caller disconnected prematurely) and the PSAP's calling number undergoes attestation/authentication in the NG9-1-1 Emergency Services Network. The RPH and SIP Priority header are also signed in the NG9-1-1 Emergency Services Network, and both the PSAP

caller identity and the RPH/Priority header fields undergo verification in the emergency caller's home network. The emergency callback is then delivered to the emergency caller with the i3 PSAP calling number.

Actors

Carol is the PSAP call-taker that is placing the emergency callback (i.e., the call-taker to which the original 9-1-1 call was delivered).

Bob is the emergency caller whose placed the original 9-1-1 call.

Pre-Conditions

Carol originates a callback call that has a 10-digit callback number associated with it.

Post-Conditions

Carol is in communication with Bob.

Normal Flow – The NG9-1-1 Emergency Services Network associates an Attestation Level of "A" with the PSAP caller identity; the caller identity, RPH and Priority header fields are successfully signed and verified; the emergency callback call is delivered to the emergency caller's UE with the PSAP calling number and associated verification status.

1. Bob originated a 9-1-1 call which was answered by Carol. Bob disconnects prematurely from that call and Carol initiates an emergency callback toward Bob. Carol's emergency callback is routed to the NG9-1-1 Emergency Services Network.
2. The NG9-1-1 Emergency Services Network receives a callback number, an appropriate RPH value, and a Priority header value of "psap-callback" with the call.
3. The NG9-1-1 Emergency Services Network performs destination routing of the callback call (e.g., at the i3 Outbound Call Interface Function [OCIF] or IMS Transit Function) and determines that the call is to be routed via an interconnecting IP network. [This network may be Bob's home network or a transit network between the NG9-1-1 Emergency Services Network and Bob's home network.]
4. Prior to routing the callback call to the interconnecting IP network, the i3 OCIF or IMS Transit Function interacts with an Authentication Service.
5. Based on interactions with an Authentication Service, an attestation level of "A" is associated with the PSAP calling number, and the calling identity (PSAP calling number) is signed. The RPH and Priority header are also signed.
6. The NG9-1-1 Emergency Services Network routes the call toward Bob's home network, passing the signed PSAP calling number and RPH/Priority header.
7. Bob's home network interacts with a Verification Service which performs verification of the signed caller identity and RPH/Priority header. In this use case, the verification is successful.
8. Bob's home network performs destination routing and delivers the callback call to Bob's UE with the PSAP calling number (and associated verifications status), and RPH and Priority header (and verification status). [Note: It is not expected that attestation information will be provided to UEs for non-emergency calls.]
9. Bob's UE displays the PSAP calling number, along with an indication of the trustworthiness of the calling number which is based on the attestation information and verification status provided in incoming signaling.
10. Bob answers the call, and he and Carol re-initiate their conversation.

Alternate Flow – The PSAP caller identity is delivered to the NG9-1-1 Emergency Services Network with a privacy indicator; the NG9-1-1 Emergency Services Network associates an Attestation Level of "A" with the PSAP caller identity; the caller identity, RPH and Priority header fields are successfully signed and verified; the verification status associated with the PSAP caller identity is delivered to the emergency caller's UE, but the calling number is not delivered/displayed to the emergency caller.

1. Bob originated a 9-1-1 call which was answered by Carol. Bob disconnects prematurely from that call and Carol initiates an emergency callback toward Bob, indicating that she wants her calling number kept private. Carol's emergency callback is routed to the NG9-1-1 Emergency Services Network.
2. The NG9-1-1 Emergency Services Network receives a callback number, an appropriate RPH value, and a Priority header value of "psap-callback" with the call.
3. The NG9-1-1 Emergency Services Network performs destination routing of the callback call (e.g., at the i3 OCIF or IMS Transit Function) and determines that the call is to be routed via an interconnecting IP network. [This network may be Bob's home network or a transit network between the NG9-1-1 Emergency Services Network and Bob's home network.]
4. Prior to routing the callback call to the interconnecting IP network, the i3 OCIF or IMS Transit Function interacts with an Authentication Service.
5. Based on interactions with an Authentication Service, an attestation level of "A" is associated with the PSAP calling number, and the calling identity (PSAP calling number), the RPH and the Priority header are signed.
6. The NG9-1-1 Emergency Services Network routes the call toward Bob's home network, passing the signed callback number and RPH/Priority header.
7. Bob's home network interacts with a Verification Service which performs verification of the signed caller identity and RPH/Priority header. In this use case, the verification is successful.
8. Bob's home network performs destination routing and delivers the emergency callback to Bob's UE. Because the PSAP's calling number is to be kept private, only the verification status associated with the PSAP calling number is delivered to Bob's UE. [Note: It is not expected that attestation information will be provided to UEs for non-emergency calls.]
9. Bob's UE displays an indication of the trustworthiness of the calling information, based on the verification status provided in incoming signaling, but does not display the calling number itself.
10. Bob answers the call, and he and Carol re-initiate their conversation.

7 Roadmap of Specifications Relevant to SHAKEN and RPH and Priority Header Signing/Verification for 9-1-1

The following specifications address topics relevant to the application of SHAKEN caller identity authentication/verification and/or RPH and Priority header signing/verification to 9-1-1 calls and callback calls.

7.1 ATIS Specifications in Support of Information Spoofing Mitigation

7.1.1 ATIS-1000074-E, Signature-based Handling of Asserted information using toKENs (SHAKEN)

ATIS-1000074-E [Ref 1] provides a framework and guidance on how to utilize 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 1] 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 1], 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 carrier of the party receiving the call to provide an indication to the called party of the legitimacy of the caller identity. Updates are being made to ATIS-1000074-E [Ref 1] to address caller identity authentication and verification associated with emergency (i.e., 9-1-1) calls and emergency callbacks initiated by PSAPs.

7.1.2 ATIS-1000080, *Signature-based Handling of Asserted information using toKENs (SHAKEN): Governance Model and Certificate Management*

ATIS-1000080 [Ref 7] introduces a governance model, certificate management architecture, and related protocols to the SHAKEN framework defined in ATIS-1000074-E [Ref 1]. The certificate management procedures identify the functional entities and protocols involved in the distribution and management of STI Certificates. The governance model identifies functional entities that have the responsibility to establish policies and procedures to ensure that only authorized entities are allowed to administer digital certificates within VoIP networks. This document provides recommendations and requirements for supporting the management of Service Provider-level certificates within the SHAKEN framework. The mechanisms defined in this document are relevant to the signing of caller identity, RPH, and Priority header information in the context of 9-1-1 calls and callback calls.

7.1.3 ATIS-1000081, *ATIS Technical Report on a Framework for Display of Verified Caller ID*

ATIS-1000081 [Ref 8] provides a framework for signaling verified caller identity information from the network to User Equipment and displaying the information on the UE in a uniform manner, independent of technology. The guidelines presented in this document are best practices based on a review of industry standards and studies addressing the effectiveness of warning signs and human factors related to the reading and comprehension of variable messages (text and symbolic). This report recommends that these guidelines be taken into consideration by all stakeholders (service providers, equipment manufacturers, and analytics providers) in the deployment of verified caller identity displays and the composition of its related messages. While the display of verified caller identity information to PSAPs in the context of 9-1-1 calls may be different than typical displays provided to called users, this document may provide a basis for the display of verified caller identity information to emergency callers in the context of callback calls.

7.1.4 ATIS-1000082, *Technical Report on SHAKEN APIs for a Centralized Signing and Signature Validation Server*

ATIS-1000082 [Ref 9] defines a Representational State Transfer (REST)ful Applications Programming Interface (API) that can be used in the context of the SHAKEN framework to sign and verify telephony identity. Because of the potential need for a service provider to initiate authentication and verification in multiple networks and/or from different network elements within their infrastructure, there is a benefit to defining an API that will allow a centralized authentication service and verification service to be called upon from various points within a service provider's infrastructure (e.g., from the network edge vs. the network core). ATIS-1000082 [Ref 9] describes a HyperText Transfer Protocol (HTTP)-based API that can be used between an "authenticator" and Signing server functions and between a "verifier" and Signature Validation server functions. The authenticator and verifier functions may be integrated into other network elements or may be developed as stand-alone functions. Based on the architecture defined in 3GPP TS 24.229 [Ref 18] for processing of emergency (9-1-1) calls in IMS networks, an HTTP-based API may be used to support the signing and verification of caller identity information associated with an emergency caller. Extensions to this API will be needed to support the signing and verification of RPH and Priority header information in support of 9-1-1 calls and callback calls.

7.1.5 ATIS-1000084, *Technical Report on Operational and Management Considerations for SHAKEN STI Certification Authorities and Policy Administrators*

ATIS-1000084 [Ref 10] introduces operational and management considerations for STI Certification Authorities (STI-CAs) within the context of the SHAKEN framework described in ATIS-1000074-E [Ref 1] and the SHAKEN: Governance Model and Certificate Management framework described in ATIS-1000080 [Ref 7]. ATIS-1000084 [Ref 10] focuses on the operational and management aspects that impact the authentication and verification services, as well as general Certification Authority (CA) practices and policies. It also addresses operational aspects of managing the list of STI-CAs and authorization of Service Providers to obtain STI certificates by the STI Policy Administrator (STI-PA). The SHAKEN Governance Model and Certificate Management framework introduces a model whereby the STI-PA maintains a list of trusted STI-CAs. This list is distributed to Service Providers and used during the verification process to ensure that the public key certificate associated with a specific SIP Identity header field has been issued by a valid STI-CA. This document specifies the form of the information stored in the list and the mechanism for distributing that list to the Service Providers. The Service Provider obtains STI certificates from

the STI-CA to create signatures authenticating itself as the signing entity and protecting the integrity of the Identity header field. The SHAKEN certificate management framework is based on using a signed Service Provider Code token for validation when requesting an STI certificate. Note that a separate PSAP Credentialing Agency (PCA) Certificate Policy is being defined by NENA to provide security requirements needed to support the secure issuance of Certificates in NG9-1-1 by the PCA CAs in the NG9-1-1 Public Key Infrastructure (PKI). The root of trust in the NG9-1-1 PKI is the PCA.

7.1.6 ATIS-1000098, *Session Initiation Protocol (SIP) Resource-Priority Header (RPH) and Priority Header Signing in Support of Emergency Calling*

ATIS-1000098 [Ref 2] leverages the SHAKEN model specified in ATIS-1000074-E [Ref 1] to cryptographically sign and verify the SIP RPH and Priority header fields associated with emergency calls and callback calls (i.e., RPH values in the “esnet” namespace and a Priority header value of “psap-callback”). Note that application of SIP RPH signing to emergency calls and SIP RPH and Priority header signing to callback calls is in addition to the caller identity authentication and verification defined in ATIS-1000074-E [Ref 1]. Cryptographically signing the SIP RPH and Priority header fields and verifying that the SIP RPH and Priority header fields can be trusted can be used to mitigate against unauthorized spoofing of or tampering with the information conveyed in the SIP RPH or Priority header fields. The framework specified in ATIS-1000098 [Ref 2] leverages the SHAKEN infrastructure for caller identity authentication and verification and describes how the PASSporT “rph” extension defined in IETF RFC 8443 [Ref 11], with the RPH assertion values and SIP Priority header claim described in draft-ietf-stir-rph-emergency-services [Ref 6], can be used for the purpose of providing a trust mechanism for the SIP RPH associated with emergency calls and the SIP RPH and Priority header associated with callback calls that cross IP Network-to-Network Interface (NNI) boundaries.

7.1.7 ATIS-0500032, *ATIS Standard for Implementation of an IMS-based NG9 1 1 Service Architecture*

ATIS-0500032 [Ref 12] applies IMS architecture concepts to 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 [Ref 12] are being developed to address the impacts on an 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 and Priority header signing associated with callback calls that are routed via an NG9-1-1 Emergency Services Network toward the emergency caller.

7.1.8 ATIS-0500036, *ATIS Standard for IMS-based Next Generation Emergency Services Network Interconnection*

ATIS-0500036 [Ref 13] 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 caller identity and RPH verification procedures associated with alternate-routed or transferred 9-1-1 calls that are passed between NG9-1-1 Emergency Services Networks.

7.1.9 ATIS-0700015, *ATIS Standard for Implementation of 3GPP Common IMS Emergency Procedures for IMS Origination and ESInet/Legacy Selective Router Termination*

ATIS-0700015 [Ref 14] defines and adapts, 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 14]

architecture and the SHAKEN infrastructure must be considered to fully support caller identity assertion/authentication and RPH signing associated with emergency calls, as well as verification of caller identity, RPH, and Priority header 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.

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

ATIS-0700048 [Ref 15] analyzes the impacts on IMS originating networks of applying SHAKEN caller identity authentication and verification, and RPH and SIP Priority header signing/verification to 9-1-1 calls and callback calls. In particular, ATIS-0700048 [Ref 15] focuses on identifying the impacts on ATIS-0700015, *ATIS Standard for Implementation of 3GPP Common IMS Emergency Procedures for IMS Origination and ESInet/Legacy Selective Router Termination* [Ref 14] associated with the application of information spoofing mitigation techniques. 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 [Ref 1].

7.2 IETF Specifications in Support of Information Spoofing Mitigation

7.2.1 IETF RFC 8224, Authenticated Identity Management in the Session Initiation Protocol (SIP)

RFC 8224 [Ref 3] defines a mechanism for securely identifying originators of SIP requests by defining a SIP header field for conveying a signature used to validate the identity and for conveying a reference to the credentials of the signer. This specification defines a logical “authentication service” that validates outgoing requests. Once the originator of the message has interacted with the authentication service and been authenticated, the authentication service creates and adds an Identity header field to the request which includes a digital signature verifying that the sending user has been authenticated and its claim of a particular identity has been authorized. The “verification service” validates the signature and enables policy decisions to be made based on the results of the validation. The protocols defined in RFC 8224 [Ref 3] provide a basis for the SHAKEN framework defined in ATIS-1000074-E [Ref 1].

7.2.2 IETF RFC 8225, *PASSporT: Personal Assertion Token*

RFC 8225 [Ref 4] defines a method for creating and validating a token that cryptographically verifies a Uniform Resource Identifier (URI) or telephone number representing an originating identity. The Personal Assertion Token (PASSporT) is cryptographically signed to protect the integrity of the identity of the originator and to verify the assertion of the identity information at the destination. The PASSporT defined in RFC 8225 [Ref 4] includes a number of claims that the signer of the token is asserting that convey the identity of the origination and destination associated with the communication. The associated public certificate is used to verify the digital signature and the claims included in the PASSporT. The goal of a PASSporT is to provide a common framework for signing information related to the originating identity in an extensible way. RFC 8224 [Ref 3] uses the PASSporT defined in RFC 8225 [Ref 4] to support the signing and verification of telephone numbers and SIP URIs.

7.2.3 IETF RFC 8558, *Personal Assertion Token (PASSporT) Extension for Signature-based Handling of Asserted information using toKENs (SHAKEN)*

In support of the SHAKEN framework defined in ATIS-1000074-E [Ref 1], RFC 8558 [Ref 16] extends the PASSporT defined in RFC 8225 [Ref 4] to include both a specific set of levels of confidence in the correctness of the originating identity of a call originated in a SIP-based telephone network, as well as an identifier that allows a Service Provider to uniquely identify the origin of the call within its network. In addition to the base PASSporT claims, RFC 8558 [Ref 16] defines two additional claims. The attestation claim indicates one of three values: full attestation (i.e. the service provider can fully attest to the calling identity); partial attestation (i.e., the service provider originated a telephone call but cannot fully attest to the calling identity); and gateway attestation (i.e., the lowest level of attestation which is applicable when a service provider receives a call from a gateway that does not support PASSporT or STI). The

second additional claim consists of a unique origination identifier used by the service provider to identify the source of a telephone call to support traceback for enforcement and identification of a source of illegitimate calls.

7.2.4 IETF RFC 8443, *Personal Assertion Token (PASSporT) Extension for Resource Priority Authorization*

RFC 8443 [Ref 11] extends the PASSporT defined in RFC 8225 [Ref 4] to allow the inclusion of cryptographically signed assertions of authorization for the values populated in the SIP RPH field. The RPH allows for prioritized access to network resources during periods of communications resource scarcity (e.g., network congestion). Like caller identity information, the SIP RPH field could be spoofed and abused by unauthorized entities, leading to the misuse of resources during periods of congestion. By signing the SIP RPH field, a receiving entity can verify the validity of assertions authorizing the SIP RPH field and act on the information with confidence that the information has not been spoofed or compromised. The PASSporT extension defined in RFC 8443 [Ref 11] provides attestation of a calling-user authorization for priority communications, in addition to the PASSporT object that is used for calling-user telephone-number attestation. RFC 8443 [Ref 11] describes an authentication that verifies a calling-user privilege for the SIP RPH field based on its identity. While not specifically addressing RPH signing in the context of emergency calling, this RFC provides a basis for the RPH and SIP Priority header signing described in draft-ietf-stir-rph-emergency-services [Ref 6].

7.2.5 IETF RFC 7090, *Public Safety Answering Point (PSAP) Callback*

Regulatory requirements demand that the emergency call setup procedure itself provides enough information to allow a PSAP call taker to initiate a callback to the emergency caller. This is desirable in those cases where the call is dropped prematurely or where further communication is necessary. A PSAP callback may, however, be blocked by user-configured authorization policies or features associated with the emergency caller that may prevent delivery of the call if SIP entities (SIP proxies as well as the SIP user equipment itself) cannot differentiate the PSAP callback from any other SIP call. RFC 7090 [Ref 5] defines a new header field value for the SIP Priority header field, called "psap-callback", that can be used to mark PSAP callbacks, potentially increasing the chances that the callback call will reach the emergency caller. RFC 7090 [Ref 5] notes that it is critical that the indicator only lead to preferential call treatment in cases where the recipient has some trust in the caller. The concept of signing a SIP Priority header with a value of “psap-callback” is addressed in draft-ietf-stir-rph-emergency-services [Ref 6].

7.2.6 IETF Internet Draft draft-ietf-stir-rph-emergency-services, *Assertion Values for a Resource Priority Header Claim and a SIP Priority Header Claim in Support of Emergency Services Networks*

Since the SIP signaling associated with 9-1-1 originations and emergency callbacks 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 calls and emergency callbacks. 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. In the context of emergency callbacks, a signed RPH would indicate that the Emergency Services Network provider asserts that they recognize the call is an emergency callback and that an appropriate RPH value should be included in the SIP signaling. As described above, RFC 7090 [Ref 5] defines the use of the SIP Priority header field set to “psap-callback” as a way of marking callback calls to facilitate special network handling of callback calls, such as bypassing services that might preclude callback calls from completing. There is currently no protection against misuse of the SIP Priority field and since, as described in RFC 7090 [Ref 5], 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 Internet Draft draft-ietf-stir-rph-emergency-services [Ref 6] defines the assertion values to be used in a Resource-Priority Header ("rph") claim in the context of emergency call originations and callbacks. IETF Internet Draft draft-ietf-stir-rph-emergency-services [Ref 6] also defines a new claim, "sph", to protect a SIP Priority header set to “psap-callback” in support of emergency callbacks.

7.3 3GPP Standards Relevant to Spoofing Mitigation for Emergency Calling

7.3.1 3GPP TS 23.167, *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS) emergency sessions*

3GPP TS 23.167 [Ref 17] defines the stage 2 service description for emergency services in the IP Multimedia Core Network Subsystem. TS 23.167 Release 16 [Ref 17] does not 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. Enhancements are needed to allow for caller identity assertion and verification associated with emergency calls and callback calls, as well as the 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. This includes scenarios where a non-dialable callback number has been associated with the emergency request.

7.3.2 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*

3GPP TS 24.229 [Ref 18] defines a call control protocol for use in the IP Multimedia (IM) Core Network (CN) subsystem based on SIP and the associated Session Description Protocol (SDP). 3GPP TS 24.229 [Ref 18] addresses calling number verification using signature verification and attestation information, as applicable to non-emergency calls. Specifically, it describes procedures at an entry Interconnection Border Control Function (IBCF) that supports calling number verification using signature verification and attestation information. TS 24.229 [Ref 18] also defines the Attestation-Info and Origination-Id header fields used in the calling number authentication process. TS 24.229 Release 16 [Ref 18] does not 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. TS 24.229 [Ref 18] Release 17 will address the application of calling number signing/verification protocol procedures to emergency originations (including scenarios where a non-dialable callback number is present) and callback calls. In addition, Release 17 of TS 24.229 [Ref 18] will address RPH signing/verification in the context of emergency calls, and RPH/Priority header signing/verification in the context of callback calls.

8 Architecture

In applying spoofing mitigation techniques, like SHAKEN, to emergency calling, it is necessary to consider the unique signaling characteristics and network architectures that are involved in supporting 9-1-1 originations and callback calls.

In keeping with the framework SHAKEN architecture described in ATIS-1000074-E [Ref 1], which shows a Call Session Control Function (CSCF) interacting with an Authentication Service in the originating network and a Verification Service (in the terminating network), initial discussions related to the architecture to support the application of SHAKEN to 9-1-1 assumed that, for 9-1-1 calls, the Emergency Call Session Control Function (E-CSCF) in the originating IMS network would interact with the Authentication Service, and an E-CSCF (in an IMS-based NG9-1-1 Emergency Services Network) or an i3 Emergency Service Routing Proxy (ESRP) (in an i3 NG9-1-1 Emergency Services Network) would interact with a Verification Service. However, 3GPP standards do not support an interface between an E-CSCF and an Application Server, such as an Authentication Service or Verification Service, and have instead defined an interface between an Interconnection Border Control Function (IBCF) and an Application Server to support the signing and verification of caller identity information. The same interfaces can be used for signing and verification of RPH information in the context of an emergency call. These are further described in Clause 8.1.

The architectures that are used to support the delivery of callback calls also have some unique characteristics. For example, multimedia callbacks that are routed via an i3 ESInet/Next Generation Core Service (NGCS) will be handled by an OCIF. Callback calls routed via an IMS-based NG9-1-1 Emergency Services Network will be handled by a Transit Function. There are multiple architectures that can be used to support the application of SHAKEN

procedures to callback calls, depending on whether the NG9-1-1 Emergency Services Network uses an i3 architecture or an IMS-based architecture. These are further described in Clause 8.2.

8.1 Reference Architectures for Caller Identity Authentication and RPH Signing/Verification Associated with 9-1-1 Calls

Figure 8.1 illustrates a reference architecture used for caller identity and SIP RPH signing/verification in the context of 9-1-1 calls where the NG9-1-1 Emergency Services Network uses a NENA i3 architecture. This architecture builds on the originating network calling number authentication/verification architecture supported by 3GPP in which an IBCF in an originating network, if configured through operator policies, invokes an Authentication Service for the signing of identity information if available in an incoming request. The IBCF then includes the signed information in the outgoing request.

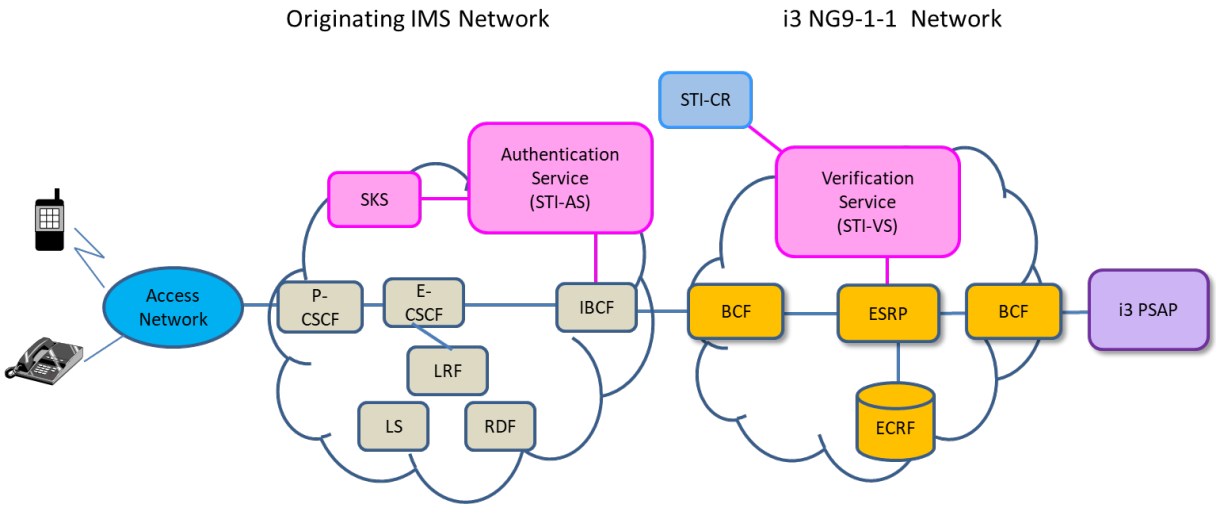

Figure 8.1: Emergency Services Initial Call Architecture with i3 NG9-1-1 Emergency Services Network

Based on the architecture illustrated in Figure 8-1, the Proxy Call Session Control Function (P-CSCF) receives the emergency call from the User Equipment via the Access Network. The P-CSCF detects that the call is an emergency call and forwards it to/toward the E-CSCF. The P-CSCF may, based on local policy, populate attestation information associated with the caller identity as well as the RPH information in the outgoing signaling to the E-CSCF. The E-CSCF receives the emergency call from the P-CSCF and interacts with a Location Retrieval Function (LRF) to obtain location and routing information for the call. The LRF obtains location information associated with the emergency call (by interacting with a Location Server [LS], if necessary) and uses that location to acquire routing information for the emergency call from the Routing Determination Function (RDF). The LRF returns location and routing information to the E-CSCF. The E-CSCF then forwards the emergency call based on the routing information. If the call is to be routed via an NG9-1-1 Emergency Services Network, the E-CSCF passes the call to an IBCF. The IBCF sends two signing requests to the Authentication Service: one associated with the caller identity and one associated with the RPH. The Authentication Service determines, through service provider-specific means, the legitimacy of the content of the caller identity and the RPH information sent to it in the signing request. The Authentication Service then securely requests its private key from the Secure Key Store (SKS). The SKS returns the private key to the Authentication Service and the Authentication Service uses it to sign the caller identity and RPH information. The Authentication Service returns two identityHeader parameters, one associated with the signed caller identity and one associated with the signed RPH, to the IBCF. The IBCF then uses the identityHeader parameters to populate SIP Identity headers in the outgoing signaling to the i3 NG9-1-1 Network.

When the ESRP in the i3 NG9-1-1 Network receives the emergency call, it passes the call signaling associated with the call to a Verification Service. The Verification Service verifies the signatures in the Identity header fields, which validate the signature associated with the caller identity and RPH field. The Verification Service passes the call signaling back to the ESRP, including an indication of the results of the verification process (i.e., verification status indicators associated with the verified caller identity and RPH). The ESRP proceeds with normal emergency call handling, using location information associated with the emergency call to query an Emergency Call Routing Function (ECRF) and using the routing information returned by the ECRF (possibly modified by policy routing rules)

to pass the call forward (via a Border Control Function [BCF]) to the i3 PSAP. The emergency call is delivered to the PSAP with the caller identity (i.e., callback) information and associated attestation level and verification results, as well as location information and the RPH (and associated verification results). The callback number (with associated attestation information and verification status) and the location information are displayed to the PSAP call taker.

Figure 8.2 illustrates a reference architecture used for caller identity and SIP RPH signing/verification in the context of 9-1-1 calls where the NG9-1-1 Emergency Services Network uses a IMS architecture.

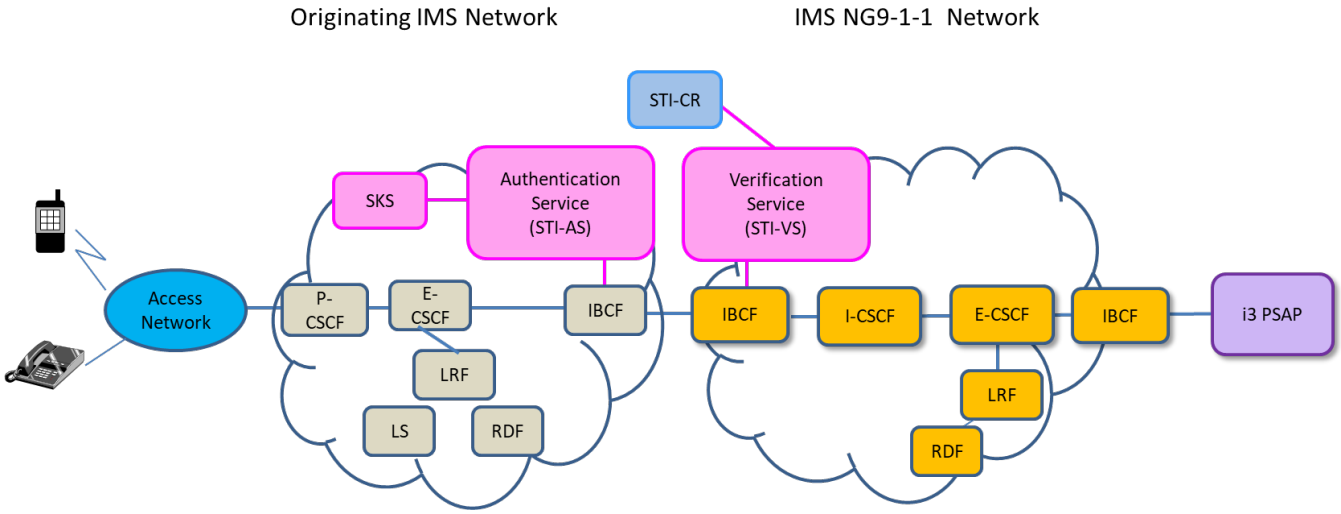

Figure 8.2: Emergency Services Initial Call Architecture with IMS NG9-1-1 Emergency Services Network

The processing of the emergency call through the originating network is the same as for Figure 8.1, however, when the call is routed forward from the originating network, it is the IBCF on the ingress side of the IMS NG9-1-1 Emergency Services Network that is responsible for interacting with the Verification Service. Instead of passing the call signaling to the Verification Service, the IBCF sends a verification request to the Verification Service that contains the Identity header information associated with the signed caller identity and the Identity header information associated with the signed RPH. As above, the Verification Service verifies the signatures associated with the signed caller identity and RPH information received by the IBCF in incoming call setup signaling. The Verification Service returns a verification response back to the IBCF that indicates the success or failure of the verification process (i.e., that includes verification status information associated with the verified caller identity and RPH). The IBCF proceeds with normal emergency call handling, passing the call via the Interrogating Call Session Control Function (I-CSCF) to the E-CSCF. As in the originating network, the E-CSCF interacts with an LRF (which in turn interacts with an LS and RDF) to obtain routing location and routing information for the call. The E-CSCF then passes the call forward via an exit IBCF to the i3 PSAP. As in the previous scenario, the emergency call is delivered to the PSAP with the caller identity (i.e., callback) information and associated attestation level and verification results, as well as location information and the RPH (and associated verification results). The callback number (with associated attestation information and verification status) and the location information are displayed to the PSAP call taker.

8.2 Reference Architecture for Caller Identity Authentication and RPH and SIP Priority Header Signing/Verification Associated with Callback Calls

Figure 8.3 illustrates a reference architecture used for caller identity, RPH, and Priority signing/verification in the context of emergency callbacks where the NG9-1-1 Emergency Services Network uses a NENA i3 architecture. This architecture assumes that callback calls are routed via an i3 OCIF which is responsible for interacting with an Authentication Service for the signing of caller identity as well as RPH and Priority header information if present in an incoming request. The OCIF then forwards the signed information to the interconnected IP network via the BCF.

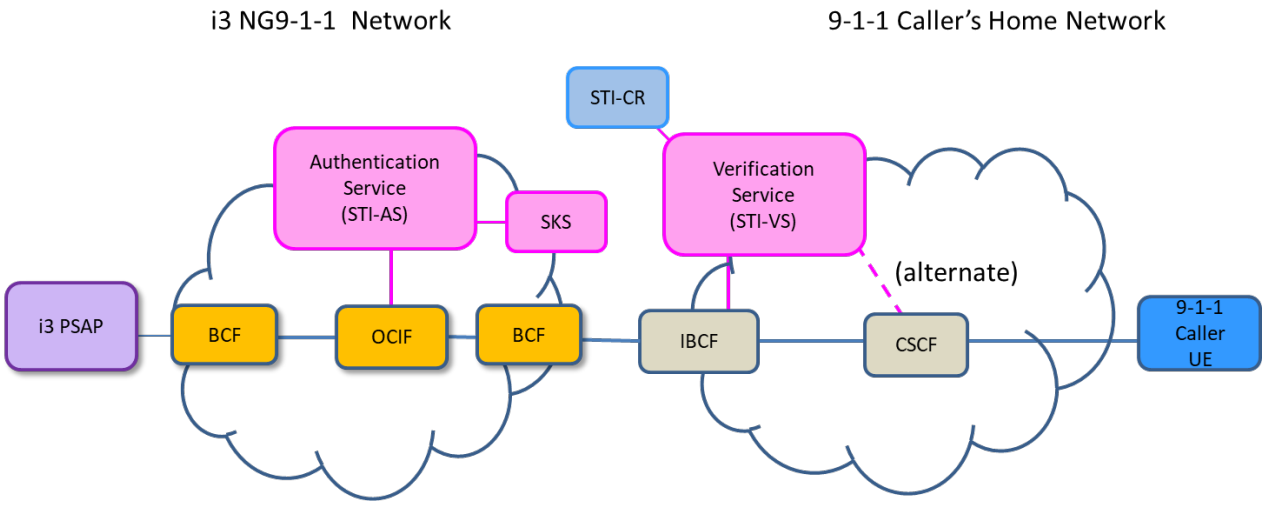

Figure 8.3: Emergency Services Callback Architecture with i3 NG9-1-1 Emergency Services Network

Based on the architecture illustrated in Figure 8.3, the i3 PSAP initiates a request for an emergency callback that includes the telephone number associated with the emergency caller to which the emergency callback is being directed, the telephone number of the PSAP that is initiating the emergency callback, a value of "psap-callback" in the Priority header field and a value of "esnet.0" in the Resource-Priority header field of the outgoing SIP signaling message. The SIP message is forwarded to the OCIF via a BCF on the ingress side of the ESInet/NGCS (possibly via an ESRP [not shown]). The OCIF uses the telephone number of the emergency caller to determine the routing for the call. In this example, the call is destined for the emergency caller's IP-based home network. Before forwarding the call to the interconnected network, the OCIF passes the SIP INVITE message to the Secure Telephone Identity Authentication Service (STI-AS) for authentication and signing of the caller identity and signing of the RPH and SIP Priority header. The STI-AS first determines through service provider-specific means the legitimacy of the PSAP telephone number identity and RPH and Priority header values included in the callback request. The STI-AS then securely requests its private key from the SKS. The SKS provides the private key in the response, and the STI-AS signs the caller identity and the RPH/Priority header. The STI-AS then adds an Identity header field associated with the caller identity and an Identity header field associated with the signed RPH/Priority header to the SIP signaling message and passes it back to the OCIF. The OCIF routes the callback call via the BCF over the NNI to the emergency caller's home network.

Figure 8.3 shows two alternatives for how the callback call will be processed by the emergency caller's home network. In one alternative, upon receiving the callback request, the IBCF at the entry point of the emergency caller's home network initiates a verification request to the Secure Telephone Identity Verification Service (STI-VS) that includes an identityHeader parameter associated with the caller identity and an identityHeaders parameter associated with the RPH/SIP Priority header. The STI-VS verifies the signatures in the identityHeader and identityHeaders parameters, 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. The STI-VS returns a verification response containing a verstatValue parameter (associated with the caller identity) and a verstatPriority parameter (associated with the RPH/SIP Priority header) to the IBCF, indicating the success or failure of the verification process. The IBCF continues to process the callback call by passing the callback request, along with the verification results, to the CSCF which passes it to the 9-1-1 caller's UE.

Figure 8.3 also illustrates an alternate flow where the entry IBCF in the emergency caller's home network forwards the callback request to the CSCF, and the CSCF passes the SIP signaling message to the STI-VS. The STI-VS performs the same verification functions as described above but populates the verification results directly in the SIP signaling message which it returns to the CSCF. The CSCF then passes the callback request to the 9-1-1 caller's UE.

Figure 8.4 illustrates a reference architecture used for caller identity and SIP RPH and Priority header signing/verification in the context of callback calls where the NG9-1-1 Emergency Services Network uses an IMS architecture. This figure shows two alternative approaches for authentication/signing of caller identity and signing of the RPH and Priority header that may be used when a callback call is routed via an IMS NG9-1-1 Emergency

Services Network. Figure 8.4 also shows two alternatives for verification of the signed caller identity and RPH/Priority header in the 9-1-1 caller's home network.

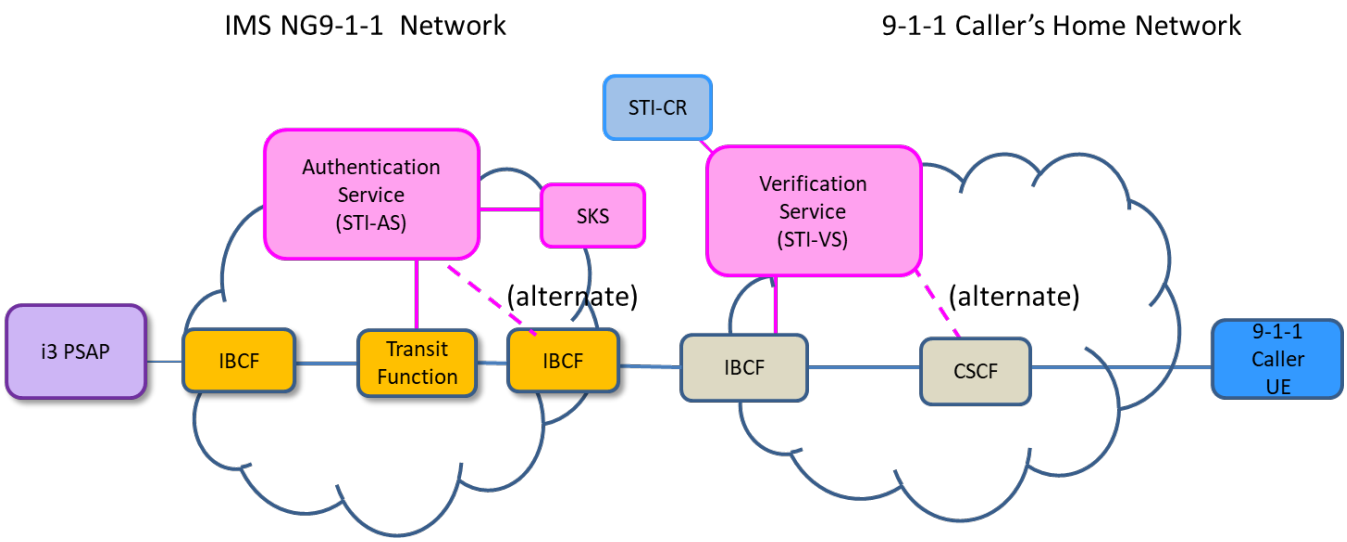

Figure 8.4: Emergency Services Callback Architecture with IMS NG9-1-1 Emergency Services Network

Based on the architecture illustrated in Figure 8.4, the i3 PSAP initiates a request for an emergency callback that includes the telephone number associated with the emergency caller to which the emergency callback is being directed, the telephone number of the PSAP that is initiating the emergency callback, a value of "psap-callback" in the Priority header field and a value of "esnet.0" in the Resource-Priority header field of the outgoing SIP signaling message. The SIP message is forwarded via an IBCF on the ingress side of the NG9-1-1 Emergency Services Network to the Transit Function. The Transit Function uses the destination address (i.e., the emergency caller's telephone number) to determine the routing for the call. In this case, the emergency caller is served by an interconnected IMS home network. In the scenario illustrated by the solid line, before forwarding the call to the 9-1-1 caller's home network, the Transit Function sends the request to the STI-AS for authentication and signing of the caller identity and signing of the RPH and Priority header content. The STI-AS determines, through service provider-specific means, the legitimacy of the telephone number identity, RPH, and Priority header associated with the emergency callback. The STI-AS is then responsible for signing the PASSporT (after interacting with the SKS to obtain the private key), adding Identity header fields and signatures (corresponding the caller identity and RPH/Priority header) to the SIP signaling message, and returning the SIP message to the Transit Function. The Transit Function passes the callback request to the exit IBCF which routes the call over the NNI toward the entry IBCF associated with the emergency caller's home network.

Figure 8.4 also illustrates an alternate flow within the IMS NG9-1-1 Emergency Services Network (illustrated by the dashed line) where the Transit Function passes the callback call (without first interacting with the authentication service) to the exit IBCF and the exit IBCF sends two signing requests to the STI-AS: one associated with the caller identity and one associated with the RPH/Priority header. The STI-AS securely obtains the private key from the SKS and uses it to sign the caller identity and RPH/Priority header information. The STI-AS returns two identityHeader parameters, one associated with the signed caller identity and one associated with the signed RPH/Priority header, to the IBCF. The IBCF uses this information to populate SIP Identity headers in the SIP signaling sent over the NNI toward the entry IBCF associated with the 9-1-1 caller's home network.

As in Figure 8.3, the architecture illustrated in Figure 8.4 supports two alternatives for which element in the 9-1-1 caller's home network interacts with the STI-VS. The solid line illustrates the scenario where the IBCF at the entry point of the emergency caller's home network initiates a verification request to the STI-VS that includes an identityHeader parameter associated with the caller identity and an identityHeaders parameter associated with the RPH/SIP Priority header. The STI-VS verifies the signatures in the identityHeader and identityHeaders parameters, which validates the caller identity and RPH/SIP Priority header field content and returns a verification response containing a verstatValue parameters (associated with the caller identity) and a verstatPriority parameter (associated with the RPH/SIP Priority header) to the IBCF, indicating the success or failure of the verification process. The IBCF continues to process the callback call by passing the callback request, along with the verification results, to the CSCF which passes it to the 9-1-1 caller's UE.

Figure 8.4 also illustrates the alternate flow where the entry IBCF in the 9-1-1 caller's home network passes the callback request to the CSCF, and the CSCF passes it to the STI-VS. The STI-VS performs the same verification functions as described above, then populates the verification results directly in the SIP signaling message that it returns to the CSCF. The CSCF then passes the callback request to the 9-1-1 caller's UE.

9 High-Level Call Flows

This section provides high-level call flows that describe the application of SHAKEN caller authentication/verification and RPH and Priority header signing/verification to 9-1-1 calls and emergency callbacks.

9.1 High-Level Call Flow for Caller Identity Authentication and RPH Signing/Verification Associated with 9-1-1 Calls Handled by an i3 NG9-1-1 Emergency Services Network

Figure 9.1 shows a call from an IMS originating network to an i3 PSAP via a NENA i3 NG9-1-1 Emergency Services Network using the reference architecture depicted in Figure 8.1. For simplification of the example, this call flow assumes that the subscriber's location is sent "by value" (i.e., location-by-value).

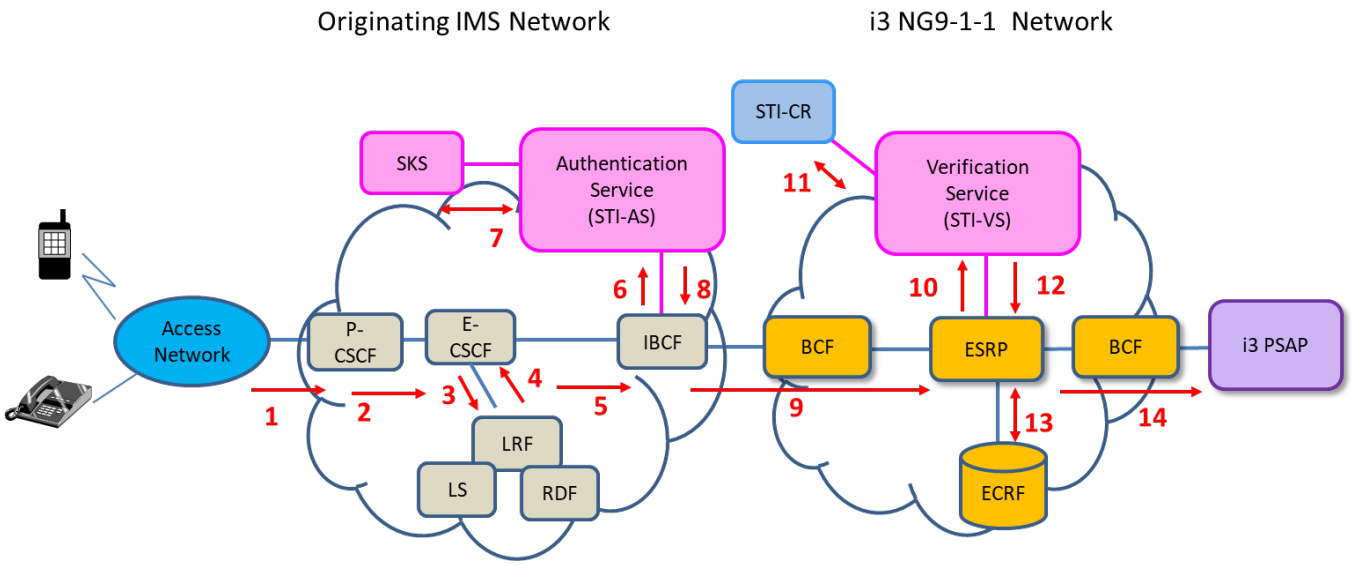

Figure 9.1: 9-1-1 Call from Originating IMS Network to i3 PSAP via an i3 NG9-1-1 Emergency Services Network

1. The call is originated and enters an IMS originating network.
2. The P-CSCF recognizes the call as an emergency call and forwards it to the E-CSCF with attestation information and an RPH populated.
3. The E-CSCF passes the call to the LRF to obtain location (if needed) and to get routing information.
4. In this example, the LRF uses the location received in incoming signaling to query the RDF for routing instructions, then returns the routing instructions to the E-CSCF.
5. The call is routed to the IBCF.
6. The IBCF sends a signing request to the Authentication Service.
7. The Authentication Service obtains its private key from the SKS.
8. The Authentication Service signs the callback number and RPH and returns the signed information to the IBCF.
9. The IBCF routes the call, with the signed callback and associated attestation information and the signed RPH, to the ESRP in the ESInet via the BCF.
10. The ESRP passes the 9-1-1 call to the Verification Service.
11. The Verification Service retrieves the certificate from the Secure Telephone Identity Certificate Repository (STI-CR) and verifies the signature associated with the callback number and RPH.
12. The Verification Service returns the call to the ESRP, along with the results of the verification process.
13. The ESRP uses the location received with the call and an appropriate service Uniform Resource Name (URN) to interrogate the ECRF for routing instructions.

14. The ESRP routes the call to the i3 PSAP, based on the routing instructions received from the ECRF and any applicable policy routing rules. The call is delivered to the i3 PSAP with location information, callback information and associated attestation information and verification status, and RPH and associated verification status.

9.2 High-Level Call Flow for Caller Identity Authentication and RPH Signing/Verification Associated with 9-1-1 Calls Handled by an IMS NG9-1-1 Emergency Services Network

Figure 9.2 shows a call from an IMS originating network to an i3 PSAP via an IMS NG9-1-1 Emergency Services Network using the reference architecture depicted in Figure 8.2. For simplification of the example, this call flow assumes that the subscriber's location is sent "by value" (i.e., location-by-value).

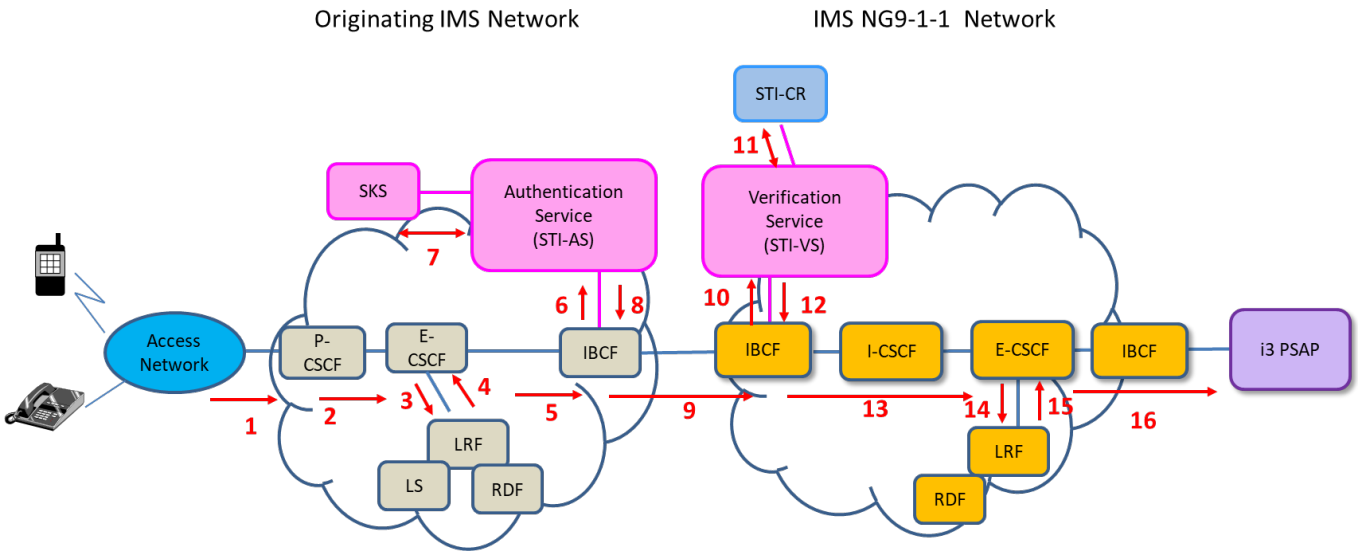

Figure 9.2: 9-1-1 Call from Originating IMS Network to i3 PSAP via an IMS NG9-1-1 Emergency Services Network

1. The call is originated and enters an IMS originating network.
2. The P-CSCF recognizes the call as an emergency call and forwards it to the E-CSCF with attestation information and an RPH populated.
3. The E-CSCF passes the call to the LRF to obtain location (if needed) and to get routing information.
4. In this example, the LRF uses the location received in incoming signaling to query the RDF for routing instructions, then returns the routing instructions to the E-CSCF.
5. The call is routed to the IBCF.
6. The IBCF sends a signing request to the Authentication Service.
7. The Authentication Service obtains its private key from the SKS.
8. The Authentication Service signs the callback number and RPH and returns the signed information to the IBCF.
9. The IBCF routes the call, with the signed callback and associated attestation information and the RPH, to an IBCF on the ingress side of the IMS NG9-1-1 Emergency Services Network.
10. The IBCF sends a verification request to the Verification Service.
11. The Verification Service retrieves the certificate from the STI-CR and verifies the signature associated with the callback number and RPH.
12. The Verification Service returns the verification status to the IBCF.
13. The IBCF passes the call, along with location information, callback information and associated attestation information and verification status, and RPH and associated verification status, to the E-CSCF via the I-CSCF.
14. The E-CSCF forwards the call to the LRF.
15. The LRF queries the RDF using the location information received with the call and an appropriate service URN. In this example, the RDF returns a route URI associated with the i3 PSAP that is served by the IMS NG9-1-1 Emergency Services Network. The LRF applies policy routing rules, as appropriate, and returns the routing instructions to the E-CSCF.

16. The E-CSCF routes the call to the i3 PSAP, based on the routing instructions received from the LRF. The call is delivered to the i3 PSAP with location information, callback information and associated attestation information and verification status, and RPH and associated verification status.

9.3 High-Level Call Flow for Caller Identity Authentication and RPH Signing/Verification Associated with Emergency Callback Handled by a NENA i3 NG9-1-1 Emergency Services Network

Figure 9.3 shows an emergency callback routed via a NENA i3 NG9-1-1 Emergency Services Network to an emergency caller served by an IMS network using the reference architecture depicted in Figure 8.3. In the example illustrated below, the OCIF in the NENA i3 NG9-1-1 Emergency Services Network is responsible for interacting with the Authentication Service and the IBCF in the emergency caller's home network is responsible for interacting with the Verification Service. Alternatively, the CSCF in the emergency caller's home network can interact with the Verification Service.

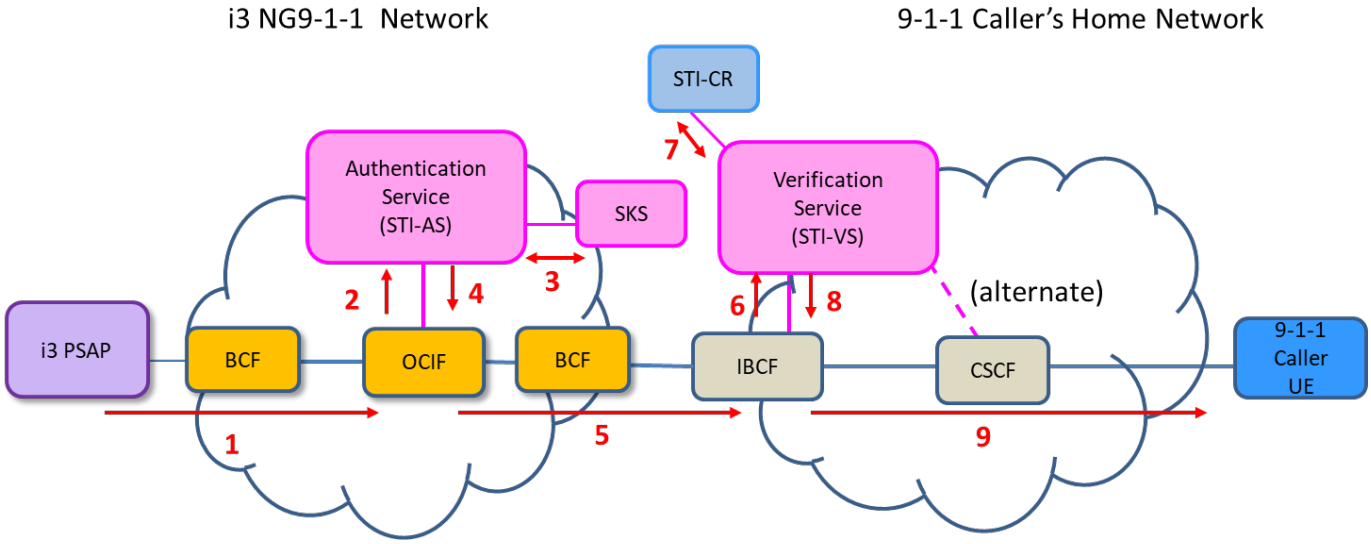

Figure 9.3: Emergency Callback Routed via a NENA i3 NG9-1-1 Emergency Services Network

1. The i3 PSAP initiates an emergency callback with the callback number associated with the emergency caller as the intended destination for the call, a calling number associated with the PSAP, an RPH, and a Priority header that marks the call as a callback call, and forwards it to the OCIF via the BCF (and optionally an ESRP [not shown]) on the ingress side of the i3 NG9-1-1 Emergency Services Network.
2. The OCIF uses the destination address (i.e., the emergency caller's callback number) to determine the routing for the call. Before forwarding the call to an interconnecting IP-capable network, the OCIF passes the emergency callback to the Authentication Service for authentication and signing of the PSAP caller identity and signing of the RPH and Priority header information.
3. The Authentication Service obtains its private key from the SKS.
4. The Authentication Service signs the PSAP caller identity, RPH, and Priority header, and returns the call with the signed information to the OCIF.
5. The OCIF routes the call, with the signed caller identity and associated attestation information, and the signed RPH and Priority header via the BCF to the entry IBCF in the interconnected network. In this example, the interconnected network is the 9-1-1 caller's home network.
6. The entry IBCF in the emergency caller's home network sends a verification request to the Verification Service that contains the signed caller identity and associated attestation level, and the signed RPH and Priority header.
7. The Verification Service retrieves the certificate from the STI-CR and verifies the signature associated with the caller identity, RPH, and Priority header.
8. The Verification Service returns the verification status to the IBCF.
9. The IBCF passes the emergency callback with the caller identity and associated attestation information and verification status, and the RPH and Priority header and associated verification status, via a CSCF to the 9-1-1 caller's UE.

9.4 High-Level Call Flow for Caller Identity Authentication and RPH Signing/Verification Associated with Emergency Callback Handled by an IMS NG9-1-1 Emergency Services Network

Figure 9.4 shows an emergency callback routed via an IMS NG9-1-1 Emergency Services Network to an emergency caller served by an IMS network using the reference architecture depicted in Figure 8.4. In the example illustrated below, the Transit Function in the IMS NG9-1-1 Emergency Services Network is responsible for interacting with the Authentication Service and the IBCF in the emergency caller's home network is responsible for interacting with the Verification Service. Using an alternative architecture in the IMS NG9-1-1 Emergency Services Network, the IBCF could interact with the Authentication Service rather than the Transit Function. An alternative architecture in the 9-1-1 caller's home network would allow the CSCF in the emergency caller's home network to interact with the Verification Service, rather than the IBCF.

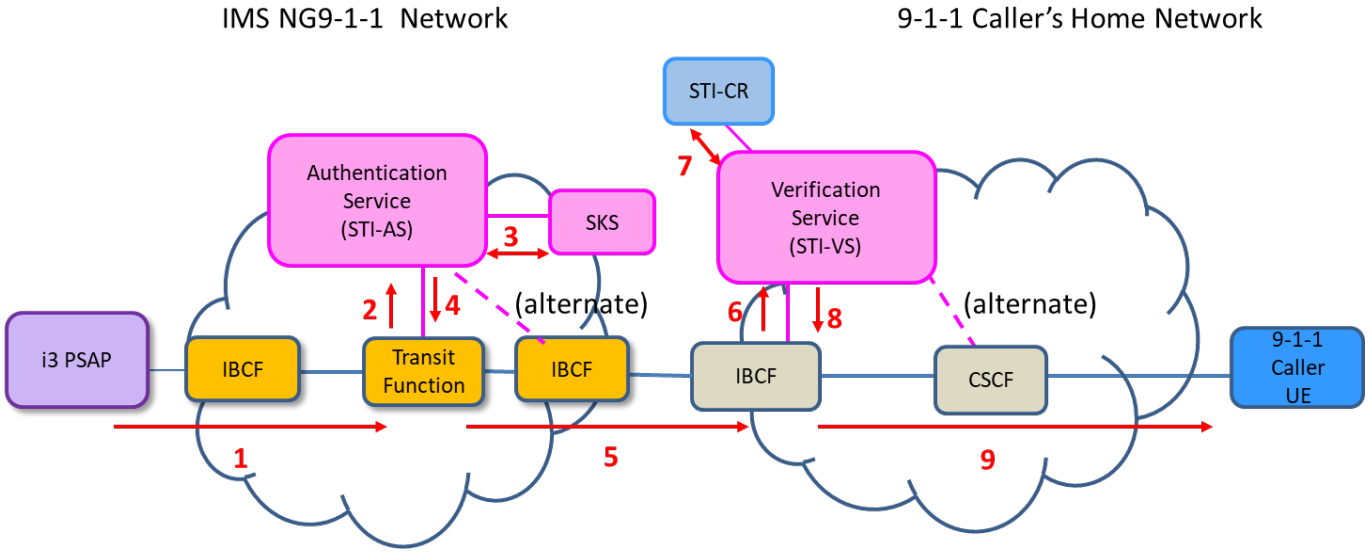

Figure 9.4: Emergency Callback Routed via an IMS NG9-1-1 Emergency Services Network

1. The i3 PSAP initiates an emergency callback with the callback number associated with the emergency caller as the intended destination for the call, a calling number associated with the PSAP, an RPH, and a Priority header that marks the call as a callback call, and forwards it to the Transit Function via an entry IBCF in an IMS NG9-1-1 Emergency Services Network.
2. The Transit Function uses the destination address (i.e., the emergency caller's callback number) to determine the routing for the call. Before forwarding the call to an interconnecting IP-capable network, the Transit Function passes the emergency callback to the Authentication Service for authentication and signing of the PSAP caller identity and signing of the RPH and Priority header information.
3. The Authentication Service obtains its private key from the SKS.
4. The Authentication Service signs the PSAP caller identity, RPH, and Priority header, and returns the call with the signed information to the Transit Function.
5. The Transit Function routes the call, with the signed caller identity and associated attestation information, and the signed RPH and Priority header, via an exit IBCF to the entry IBCF in the interconnected network. In this example, the interconnected network is the 9-1-1 caller's home network.
6. The entry IBCF sends a verification request to the Verification Service that contains the signed caller identity and associated attestation level, and the signed RPH and Priority header.
7. The Verification Service retrieves the certificate from the STI-CR and verifies the signature associated with the caller identity, RPH, and Priority header.
8. The Verification Service returns the verification status to the IBCF.
9. The IBCF passes the emergency callback with the caller identity and associated attestation information and verification status, and the RPH and Priority header and associated verification status, via a CSCF to the 9-1-1 caller's UE.

10 Handling of Calls with Non-Dialable Callback Numbers

The application of SHAKEN caller identity authentication/verification to 9-1-1 calls must address the handling of 9-1-1 originations where the caller identity is in the form of a non-dialable callback number. J-STD-036-C-2 [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 (e.g., non-initialized mobile devices, mobile phones whose subscription has expired, mobile phones that fail authentication, mobile phones without a subscriber identity module inserted, “9-1-1 Only” devices). In scenarios where a non-dialable callback number is appropriate, J-STD-036-C-2 [Ref 19] 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”. If an emergency call is initiated using one of the devices described above, and the originating network handling the call is an IMS network, the E-CSCF will be responsible for inserting a non-dialable callback number in the P-Asserted-Identity header of the SIP INVITE message, formatted as described in J-STD-036 [Ref 19], into the SIP signaling associated with the call. If the IMS originating network determines that the emergency call is to be routed to an IP/SIP-capable NG9-1-1 network (IMS-based or NENA i3 ESInet/NGCS), the call will be forwarded from the E-CSCF to an exit IBCF in the IMS originating network before being passed to the NG9-1-1 Emergency Services Network, with the non-dialable callback number included in the SIP signaling. As illustrated in Figure 8.1, when an exit IBCF receives a SIP INVITE associated with a 9-1-1 call, it will send a signing request to the Authentication Service to request signing of the caller identity. The signing request will typically include an ‘attest’ parameter indicating the attestation level associated with the caller identity. If the caller identity information is a non-dialable callback number that has been populated by the originating network E-CSCF, then the signing request sent by the exit IBCF to the Authentication Service will include 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, additional clarifications need to be made to the Authentication Service and Verification Service, as described in ATIS-1000074-E [Ref 1], to address scenarios where an emergency call has a non-dialable callback number. Specifically, 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 will 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 must be updated 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 will canonicalize the calling TN to remove any leading '+' sign or visual separators, and use the resulting digit-string to check the "orig" claim. This special procedure will only be applied if the non-dialable callback number is a string of 10 digits with leading digits "911" or 11 digits with leading digits "1911".

11 Operational Considerations

The application of spoofing mitigation techniques to 9-1-1 calls and emergency callbacks will have operational impacts on IMS originating networks, NG9-1-1 Emergency Services Networks, and especially i3 PSAPs. This clause describes the operational considerations associated with these components of the NG9-1-1 service architecture.

11.1 IMS Originating Networks

IMS originating networks play a critical role in caller identity authentication and RPH signing associated with 9-1-1 calls, but there are aspects of the SHAKEN spoofing mitigation mechanism that are currently left to local policy, leading to operational implications. For example, as described in Clause 8.1, a P-CSCF in an IMS originating network, upon detecting an emergency call may, based on local policy, populate attestation information associated with the calling identity as well as the RPH information in the outgoing signaling to the E-CSCF. In addition, ATIS-1000074-E [Ref 1] indicates that the Authentication Service provided by the STI-AS determines *through service provider-specific means* the legitimacy of the calling identity associated with the call.

At a minimum, there are configuration- and provisioning-related impacts associated with functionality supported by the P-CSCF in handling 9-1-1 calls within IMS originating networks where SHAKEN and RPH signing are supported. For example, if the P-CSCF is responsible for performing attestation of the caller identity associated with a 9-1-1

call, there will likely be operational impacts associated with defining the criteria that the P-CSCF uses in determining what attestation level should be populated in outgoing SIP signaling associated with the call.

If local policy dictates that the P-CSCF should not populate information like the attestation level or RPH, there are downstream implications. For example, an IBCF that receives SIP signaling associated with a 9-1-1 call may be responsible for interacting with the Authentication Service to authenticate/sign the callback number and RPH. If the P-CSCF does not populate an Attestation-Info parameter in the SIP signaling, the IBCF will need to use other means (e.g., provisioned data) to determine how to populate the “attest’ parameter in the signing request associated with the caller identity that it sends to the Authentication Service. If the IBCF does not receive an RPH in incoming SIP signaling associated with a 9-1-1 call, it will not send an RPH-related signing request to the Authentication Service. In addition, an i3 BCF or IBCF on the ingress side of the NG9-1-1 Emergency Services Network will be responsible for populating an appropriate RPH value in the SIP signaling associated with the 9-1-1 call.

Call Detail Records (CDRs) will need to capture information about calling number authentication information in SIP call signaling. CDRs should include information such as: the SHAKEN Identity header and/or RPH that was associated with the call; the interface over which the call was received; an indication of the attestation level associated with the call; an indication of whether the authentication process was successful.

11.2 NG9-1-1 Emergency Services Networks

Several aspects of the caller identity/RPH verification process associated with 9-1-1 calls are left to local policy, potentially having configuration/provisioning impacts. For example, a determination by the Verification Service accessed by an element in the NG9-1-1 Emergency Services Network of whether the “Issued At” value in an Identity header conveying PASSporT information is associated with a “fresh” certificate will be based on locally determined freshness criteria. Call handling (i.e., whether the call should continue to be processed or terminated) and other reporting in the case of verification failure is also locally determined and will likely have configuration/provisioning implications. Local policy is used to determine whether the Verification Service accessed by an NG9-1-1 Emergency Services Network interacts with Call Validation Treatment (CVT).

It is expected that logging of information associated with 9-1-1 calls will include information related to spoofing mitigation (e.g., the Identity header(s) associated with the call). NG9-1-1 Emergency Services Network providers will also be expected to initiate off-line activity, such as opening a trouble ticket, to address the cause of any verification errors.

In the context of processing emergency callbacks, local policy will determine whether an entry IBCF in an IMS NG9-1-1 Emergency Services Network adds an Origination-Id header and/or an Attestation-Info header to the SIP signaling to indicate from where the request was received. In addition, the element within an IMS NG9-1-1 Emergency Services that is responsible for interacting with an Authentication Service will depend on local policy. The NG9-1-1 Emergency Services Network must be configured properly to support the implementation of these local policies. There may also be operational impacts associated with defining the criteria that is used by the Authentication Service or the entry IBCF to determine what attestation level should be associated with the caller (i.e., PSAP) identity for an emergency callback. There are also operational considerations associated with administering the certificates used in signing caller identity, RPH and Priority header information associated with emergency callbacks.

As for 9-1-1 calls, it is expected that information associated with emergency callbacks that traverse an NG9-1-1 Emergency Services Network will be logged.

11.3 i3 PSAPs

The application of spoofing mitigation techniques to 9-1-1 calls will result in new information being made available to PSAP call takers. Standard Operating Procedures (SOPs) will need to be defined or enhanced to address the manner in which the information available as a result of spoofing mitigation will influence call handling or support post-processing associated with 9-1-1 calls. These SOPs will need to clearly define how SHAKEN-related information (e.g., attestation level) should be used by a PSAP call taker in the course of handling an emergency call and describe how an agency will prioritize and handle calls of different attestation levels in relation to other calls occurring around the same time. SOPs should identify which of the received call-related information should be recorded and should specify the processes and procedures for preserving forensic information for potential future litigation, following "chain of custody”.

It is expected that when SHAKEN is applied to a 9-1-1 call, attestation information and an indication of the verification status associated with the callback number will be displayed to the PSAP call taker, if available. The ability to display SHAKEN-related information to call takers will be constrained by PSAP equipment limitations.

Enhancements to existing PSAP equipment may be needed to accommodate the display of additional call-related information. New Methods and Procedures will need to be defined to specify how SHAKEN-related information should be used by a PSAP in the course of handling an emergency call and call takers will need to be trained to work with the new information and to recognize where it will appear on the new displays.

Since spoofing mitigation techniques may also be applied to outgoing calls from PSAPs, SOPs should define the mechanism by which a PSAP call taker can request the establishment of an outgoing call (i.e., callback call, official call, or non-official call). Based on local policy, SOPs may also provide guidance to PSAPs regarding the network or network type over which specific types of outgoing calls should be routed (i.e., whether the call should be routed via an NG9-1-1 Emergency Services Network, a VoIP carrier network, or the PSTN, as well as the conditions under which this should be done, and the specific procedures, if any, that should be used by the PSAP to trigger this routing). SOPs may also specify what calling number(s) should be used by the PSAP for a particular type of outgoing call and should provide guidance as to whether, or under what conditions, the PSAP caller identity should be kept private when generating an outgoing call.

12 Conclusion

This Technical Report describes the impacts of applying SHAKEN caller identity authentication and verification and RPH and SIP Priority header signing/verification on the processing of 9-1-1 calls and emergency callbacks to prevent malicious spoofing of caller identity, RPH and SIP Priority header information. For 9-1-1 calls, SHAKEN authentication and verification will allow attestation level and verification status information, indicating the trustworthiness of the caller identification information, to be delivered to PSAPs along with the callback number. For emergency callbacks, authentication and verification of caller identity, RPH, and Priority header information (which is used to mark a call as an emergency callback), may improve the chances of emergency callbacks being answered.

Since, like caller identity information, RPH and Priority header information could be spoofed, a signed SIP RPH and Priority header will allow a receiving entity to verify the assertion of information in the SIP RPH and Priority header fields, providing assurance that the information has not been spoofed or compromised. Emergency Services Network providers and home networks serving emergency callers will benefit from knowing whether the RPH and Priority header accompanying a 9-1-1 or callback call can be trusted before applying special processing or routing to such calls.

This Technical Report also provides a roadmap to the various standards/specifications that address topics relevant to the application of SHAKEN caller identity authentication/verification and/or RPH and Priority header signing/verification to 9-1-1 calls and callback calls. The specifications described in Clause 7 provide the building blocks for the capabilities described in this document, as well as highlighting the need for additional activity within ATIS, IETF, and 3GPP to fully support the application of caller identity authentication/verification and RPH and Priority header signing/verification to 9-1-1 calls and callback calls.

Finally, this Technical Report highlights the operational impacts associated with the application of information spoofing mitigation techniques to 9-1-1 and callback call processing. Providers of originating networks and NG9-1-1 Emergency Services Networks will have to configure their networks to reflect their local policies with regard to the elements responsible for interacting with Authentication and Verification services, and the criteria used for determining attestation levels and validating caller identity and other call-related information. Consideration must also be given to establishing mechanisms to support the logging of call-related information, including information resulting from the application of spoofing mitigation mechanisms to 9-1-1 calls and emergency callbacks,

For i3 PSAPs, operational considerations include the development or enhancement of SOPs to guide call takers in using the new information that may be available to them as a result of applying spoofing mitigation techniques when handling 9-1-1 calls. Guidance with regard to the establishment of outgoing calls that may be subject to spoofing mitigation should also be provided to PSAPs via defined policies and SOPs.

While significant progress has been made in defining architectures, procedures, and protocols to support the application of information spoofing mitigation techniques, such as SHAKEN and RPH and Priority header signing/verification to 9-1-1 calls and emergency callbacks, standards development activities are ongoing. The feasibility of applying spoofing mitigation techniques to other information that is important to 9-1-1 call handling, such as location information, should also be explored.