NENA Spoofing Mitigation Information Document

Abstract: This Information Document describes the application of the Signature-based Handling of Asserted Information Using toKENs (SHAKEN) caller identity spoofing mitigation framework and SIP Resource-Priority Header and Priority header signing/verification procedures to 9-1-1 calls and emergency callbacks in an end-state Next Generation 9-1-1 (NG9-1-1) (i.e., all-Internet Protocol [IP]) environment as well as caller identity spoofing mitigation mechanisms applicable to an all-Time Division Multiplexing (TDM) and mixed TDM/IP environment, with a focus on associated operational impacts and considerations. This Information Document also describes location spoofing mitigation in an end-state NG9-1-1 environment.

NENA Spoofing Mitigation Information Document

NENA-INF-043.3-2024
DSC Approval: January 27, 2024
PRC Approval: March 28, 2024
NENA Board of Directors Approval: April 17, 2024
Next Scheduled Review Date: April 17, 2027

Prepared by:
National Emergency Number Association (NENA) PSAP Logistics Committee, Spoofing Mitigation Working Group

1 Executive Overview

Recent regulatory activity in North America (U.S. and Canada) has had a strong emphasis on combatting nuisance calls, including robocalls and calls with illegitimate caller identity spoofing. This activity has focused on the use of caller authentication techniques based on the Signature-based Handling of Asserted Information Using toKENs (SHAKEN) standards developed by the Alliance for Telecommunications Industry Solutions (ATIS), as well as specifications developed by the Internet Engineering Task Force (IETF) Secure Telephone Identity Revisited (STIR) Working Group (WG) for calls processed in an all-Internet Protocol (IP) environment. Recent regulations have also addressed support for caller authentication in non-IP voice service provider networks as a means of addressing caller identity spoofing in an all-Time Division Multiplexing (TDM) or mixed TDM/IP environment.

Concerns regarding the illegitimate spoofing of information that is critical to the handling of emergency calls and callback calls may be addressed by applying the SHAKEN caller identity spoofing mitigation framework as well as Session Initiation Protocol (SIP) Resource-Priority Header (RPH) and Priority header signing and verification procedures to 9-1-1 calls and emergency callbacks in an end-state (all-IP) NG9-1-1 environment. 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 Public Safety Answering Points (PSAPs) along with the callback number. It is important to emphasize that the SHAKEN verification process confirms the identity of the signer of the caller identity information; *it does not specifically verify the caller identity itself*. In other words, the verification process does not guarantee that the telephone number is that of the caller, only that the Originating Service Provider says that the use of the telephone number by the caller is legitimate. As such, a service provider's reputation will depend on how rigorous they have been in asserting that a caller has a legitimate right to use a telephone number.

For emergency callbacks, authentication and verification of caller identity and Priority header information (which is used to mark a call as an emergency callback), may improve the chances of emergency callbacks being answered. The marking of the call as a "psap-callback" using the Priority header can influence how the call is processed in the 9-1-1 caller's home network, allowing the call to bypass certain features that might normally preclude the call from completing to the 9-1-1 caller.

Before the evolution to end-state NG9-1-1 is complete, 9-1-1 calls may continue to be processed using a legacy E9-1-1 architecture or a transitional NG9-1-1 architecture comprised of a combination of legacy/TDM and IP/SIP-based components. During the evolution to NG9-1-1, emergency callbacks may be originated by legacy or Next Generation (NG)/i3 PSAPs, and may traverse the legacy Public Switched Telephone Network (PSTN) or a combination of legacy and Voice over Internet Protocol (VoIP) networks prior to being delivered to the emergency caller. Solutions for supporting non-IP caller authentication in the context of 9-1-1 must take into consideration the unique signaling characteristics and network architectures that support 9-1-1 calling in a legacy or transitional environment. As a result, the non-IP caller authentication solutions being developed for non-emergency calls may not be feasible in the context of 9-1-1. For example, while the non-IP caller authentication solutions currently under discussion within the industry assume that non-IP networks support Signaling System No. 7 (SS7) signaling, there are still 9-1-1 implementations that use Multi-Frequency (MF) signaling between wireline end offices or Mobile Switching Centers (MSCs) and Selective Routers (SRs), and MF interfaces are also typically used to deliver 9-1-1 calls to legacy PSAPs. In addition, solutions that would require enhancements to SR call processing or interfaces to support caller authentication are not viewed as technically feasible.

It is critical that Public Safety have input into standards development activities associated with spoofing mitigation techniques to ensure that the operational needs of 9-1-1 Authorities/Public Safety Answering Points (PSAPs) are supported by the standards that ultimately get generated. To this end, this Information Document addresses operational as well as technical impacts associated with applying information spoofing mitigation techniques to 9-1-1 calls and emergency callbacks. Specifically, this Information Document discusses the need for spoofing mitigation to be addressed in Standard Operating Procedures (SOPs) to influence call handling and/or to support post-processing associated with emergency calls, depending on the jurisdiction. For example, SOPs must clearly define how caller authentication information (e.g., attestation level) will be displayed to PSAP call takers and describe how the information should be used in the course of handling an emergency call. SOPs should also provide guidance with respect to how an agency will prioritize and handle calls of different attestation levels relative to other calls occurring around the same time.

In addition to describing operational impacts associated with the application of spoofing mitigation techniques to 9-1-1 calls and emergency callbacks, this Information Document provides background on regulatory drivers behind the specification of spoofing mitigation activities, describes use cases in which the application of spoofing mitigation techniques may assist Public Safety agencies in detecting and mitigating Telephony Denial Of Service (TDoS) and swatting attacks, and identifies open issues that still need to be addressed.

Version 1 of this Information Document addressed spoofing mitigation associated with 9-1-1 calls and callback calls in an all-IP environment. Version 2 of this Information Document considered spoofing mitigation associated with 9-1-1 calls and callback calls in E9-1-1 and transitional NG9-1-1 environments. Specifically, Version 2 of this Information Document presented two technically viable options for explicitly conveying attestation level and verification status information to legacy PSAPs via the ALI interface. This document notes that, while ALI interface standards exist (e.g., NENA-STA-015.10-2018 [17], NENA 04-005 [18]), implementations reflect many local variations of these standards. In addition, the amount of space available and the configuration used on Customer Premises Equipment (CPE) to display call-related information to PSAP call takers varies based the type of equipment deployed. Agencies or 9-1-1 Authorities may place different priorities on the information that is displayed to call takers, making a single solution for providing attestation level and verification status information to PSAP call takers unlikely. An objective of Version 2 of this Information Document was to provide Public Safety with the tools to convey caller authentication information to legacy PSAPs, should a 9-1-1 Authority or Public Safety agency determine it is desirable to do so.

Version 3 of this Information Document discusses the signing and verification of location information provided with 9-1-1 calls in an end-state NG9-1-1 environment to assist PSAPs in identifying potential spoofing of the location information delivered with 9-1-1 calls and provided in response to location dereference requests. In addition, while outside the realm of location spoofing mitigation, Version 3 of this Information Document discusses the application of consistency checks to location information to assess the reasonableness of the location information available with 9-1-1 calls.

Table of Contents

NENA
INFORMATION DOCUMENT
NOTICE

This Information Document (INF) is published by the National Emergency Number Association (NENA) as an information source for 9-1-1 System Service Providers, network interface vendors, system vendors, telecommunication service providers, and 9-1-1 Authorities. It is not intended to provide complete design or operation specifications or parameters or to assure the quality of performance for systems that process such equipment or services.

NENA reserves the right to revise this Information Document for any reason including, but not limited to:

- Conformity with criteria or standards promulgated by various agencies,
- Utilization of advances in the state of the technical arts,
- Reflecting changes in the design of equipment, network interfaces, or services described herein.

This document is an information source for the voluntary use of communication centers. It is not intended to be a complete operational directive.

It is possible that certain advances in technology or changes in governmental regulations will precede these revisions. All NENA documents are subject to change as technology or other influencing factors change. Therefore, this NENA document should not be the only source of information used. NENA recommends that readers contact their 9-1-1 System Service Provider (9-1-1 SSP) representative to ensure compatibility with the 9-1-1 network, and their legal counsel to ensure compliance with current regulations.

Patents may cover the specifications, techniques, or network interface/system characteristics disclosed herein. No license expressed or implied is hereby granted. This document shall not be construed as a suggestion to any manufacturer to modify or change any of its products, nor does this document represent any commitment by NENA or any affiliate thereof to purchase any product whether or not it provides the described characteristics.

By using this document, the user agrees that NENA will have no liability for any consequential, incidental, special, or punitive damages arising from use of the document.

NENA's Committees have developed this document. Recommendations for changes to this document may be submitted to:

National Emergency Number Association
1700 Diagonal Rd, Suite 500
Alexandria, VA 22314
202.466.4911

or commleadership@nena.org

2 Document Conventions

NENA: The 9-1-1 Association improves 9-1-1 through research, standards development, training, education, outreach, and advocacy. Our vision is a public made safer and more secure through universally-available state-of-the-art 9-1-1 systems and better-trained 9-1-1 professionals. Learn more at https://www.nena.org.

2.1 NENA Intellectual Property Rights (IPR) and Antitrust Policy

NOTE – The user's attention is called to the possibility that compliance with this document may require use of an invention covered by patent rights. By publication of this document, NENA takes no position with respect to the validity of any such claim(s) or of any patent rights in connection therewith. If a patent holder has filed a statement of willingness to grant a license under these rights on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such a license, then details may be obtained from NENA by contacting the Committee Resource Manager identified on NENA's website at https://www.nena.org/ipr.

Consistent with the NENA IPR Policy, available at www.nena.org/ipr, NENA invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement any standards referenced by this document or to implement or follow any recommended best practices, procedures or architectures contained herein.

Please address the information to:

National Emergency Number Association
1700 Diagonal Rd, Suite 500
Alexandria, VA 22314
202.466.4911
or commleadership@nena.org

2.2 Reason for Issue/Reissue

NENA reserves the right to modify this document. Upon revision, the reason(s) will be provided in the table below.

Document Number	Approval Date	Reason For Issue/Reissue
NENA-INF-043.1-2021	August 11, 2021	Initial Document
NENA-INF-043.2-2022	April 18, 2022	Scope expanded to address spoofing mitigation in legacy E9-1-1 and transitional NG9-1-1 environments

Document Number	Approval Date	Reason For Issue/Reissue
NENA-INF-043.3-202Y	April 17, 2024	Scope expanded to address location spoofing mitigation in an end-state NG9-1-1 environment

3 Introduction

Illegitimate caller identity spoofing is a growing concern for North American telephone service providers and their customers. With the introduction of Internet Protocol (IP)-based telephony, caller identity spoofing is easier and more affordable than ever before. To combat illegal spoofing, the industry has developed standards for the authentication and verification of caller identity information for calls carried over an IP network using the Session Initiation Protocol (SIP). The Signature-based Handling of Asserted Information Using toKENs (SHAKEN) standards developed by the Alliance for Telecommunications Industry Solutions (ATIS), as well as specifications developed by the Internet Engineering Task Force (IETF) Secure Telephone Identity Revisited (STIR) Working Group (WG), allow calls traveling through interconnected carrier networks to 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 information.

There is value in applying the SHAKEN authentication and verification services and associated protocols to 9-1-1 calls as well as to emergency callbacks. For emergency (9-1-1) originations, interactions between originating network elements and the SHAKEN authentication service to support caller identity assertion and interactions between elements of the NG9-1-1 Emergency Services Network and the SHAKEN verification service, will allow verification status information, indicating the trustworthiness of the caller identification (e.g., the emergency caller's callback number) information, to be delivered to PSAPs along with the callback number. Additionally, interactions with the SHAKEN architecture and procedures to support caller authentication associated with emergency callbacks that are routed via a Next Generation 9-1-1 (NG9-1-1) Emergency Services Network, with verification provided by the emergency caller's home network, may increase the chance of the call completing to the called party, which is an important feature for emergency callbacks. The ability to recognize spoofed caller identities may provide Public Safety a critical tool to support the detection and mitigation of Telephony Denial Of Service (TDoS) attacks, as well as swatting and ransomware calls.

In addition to the caller identity authentication/verification provided by the SHAKEN framework, 9-1-1 calls and emergency callbacks may also be subject to RPH signing and verification. The SIP RPH field may be used by SIP user agents, including Public Switched

Telephone Network (PSTN) gateways, terminals, and SIP proxy servers to influence the prioritization of resources afforded to certain types of communication sessions. 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 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. A signed RPH would also convey to the Emergency Services Network provider that they can trust that the RPH was populated by the originating service provider, as opposed to being inserted by a threat agent. 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. This would indicate to the emergency caller's service provider that they can trust that the RPH was populated by an authorized entity.

This document describes the application of the SHAKEN caller identity spoofing mitigation framework and RPH signing/verification procedures to 9-1-1 calls and emergency callbacks, and identifies associated operational impacts and considerations. Recommendations regarding Standard Operating Procedures associated with the handling of caller identity attestation and verification status information are also provided.

Implementation of the SHAKEN framework by all originating and terminating voice service providers in the IP portions of their networks has been mandated by the Federal Communications Commission (FCC). It is the view of the FCC that widespread implementation of SHAKEN will not only benefit American consumers, but will also provide significant benefits to public safety by decreasing disruptions to emergency communications systems, saving lives.

In addition to mandating support for SHAKEN in IP-capable voice service provider networks, the FCC has also placed requirements on voice service providers to support call authentication in the non-IP portions of their networks. This support can be achieved either by having voice service providers upgrade the non-IP portions of their networks to support IP/SIP and then implementing SHAKEN, or by participating in industry activities focused on the development and/or testing of non-IP caller identity authentication solutions.

Most recently, the FCC has extended requirements for supporting SHAKEN caller identity authentication to Gateway Providers. See Section 3.1.1.6 for further discussion.

Key FCC activities related to caller identity spoofing mitigation are described in more detail below.

3.1 Overview of Regulatory Activities Related to Caller Identity Spoofing Mitigation

Regulatory activity in the U.S. and Canada has had a strong emphasis on combatting nuisance calls, including robocalls and calls with illegitimate caller identity spoofing. Section 3.1.1 describes the relevant regulatory activity that has taken place in the U.S., and Section 3.1.2 summarizes relevant regulatory activity in Canada.

3.1.1 Regulatory Activities in the U.S.

Regulatory concerns related to robocalling and caller identity spoofing can be traced back to the 1991 Telephone Consumer Protection and Truth in Caller ID Act (TCPA) [2]. More recently, the need to protect consumers from illegal caller identity spoofing has been a focus of activity in the FCC as well as in Congress. In July 2017, the FCC released a Notice of Inquiry [3], launching a broad inquiry into caller identity authentication and how to expedite its development and implementation. In February 2018, the FCC directed the Call Authentication Trust Anchor Working Group of the North American Numbering Council (NANC) to recommend a timeline or set of milestones for adoption and deployment of the SHAKEN call authentication mechanism. In May 2018, the NANC recommended that companies capable of signing and validating Voice over IP (VoIP) calls using the SHAKEN framework should implement SHAKEN within a period of approximately one year's time. In November 2018, FCC Chairman Pai sent letters to major voice service providers urging them to implement a robust caller identity authentication framework by the end of 2019. In June 2019, the FCC adopted a Declaratory Ruling and Third Further Notice of Proposed Rulemaking [4] that proposed and sought comment on mandating implementation of SHAKEN in the event that major voice service providers did not voluntarily implement the framework by the end of 2019. A subsequent Report and Order and Further Notice of Proposed Rulemaking (FNPRM) [5] issued on March 31, 2020, set required timelines for implementation of STIR/SHAKEN.

Key regulatory activities related to caller identity spoofing and robocalling mitigation are summarized below.

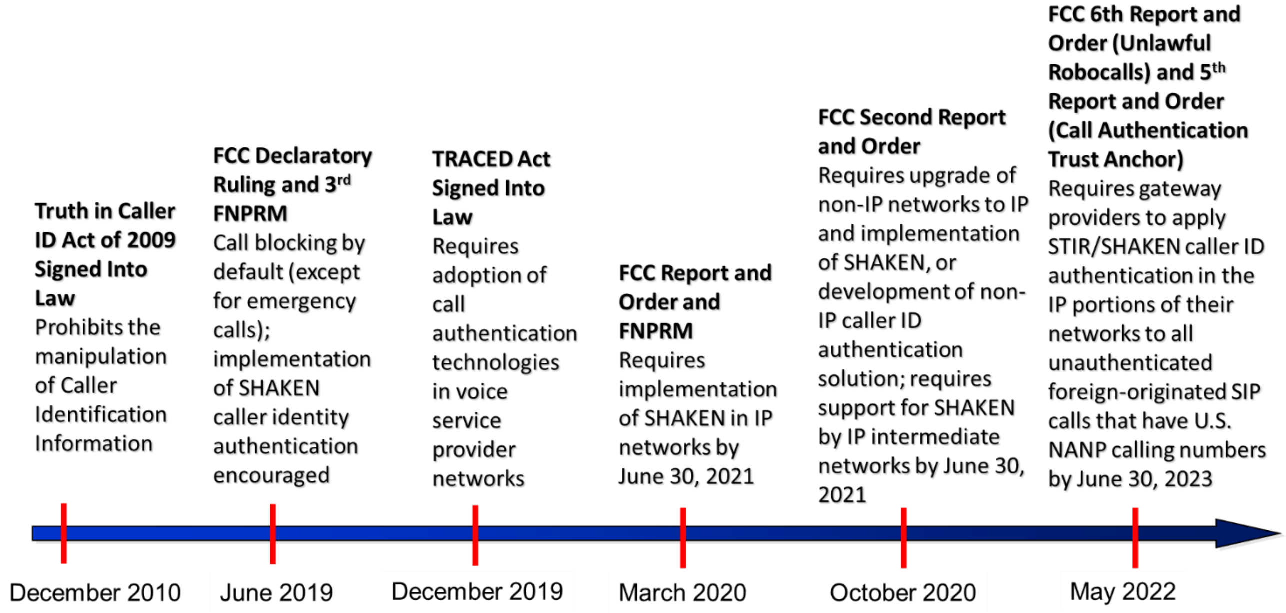

Truth in Caller ID Act of 2009 Signed Into Law
Prohibits the manipulation of Caller Identification Information
FCC Declaratory Ruling and 3rd FNPRM
Call blocking by default (except for emergency calls); implementation of SHAKEN caller identity authentication encouraged
TRACED Act Signed Into Law
Requires adoption of call authentication technologies in voice service provider networks
FCC Report and Order and FNPRM
Requires implementation of SHAKEN in IP networks by June 30, 2021
FCC Second Report and Order
Requires upgrade of non-IP networks to IP and implementation of SHAKEN, or development of non-IP caller ID authentication solution; requires support for SHAKEN by IP intermediate networks by June 30, 2021
FCC 6th Report and Order (Unlawful Robocalls) and 5th Report and Order (Call Authentication Trust Anchor)
Requires gateway providers to apply STIR/SHAKEN caller ID authentication in the IP portions of their networks to all unauthenticated foreign-originated SIP calls that have U.S. NANP calling numbers by June 30, 2023
December 2010
June 2019
December 2019
March 2020
October 2020
May 2022

Figure 3-1 Timeline of Regulatory Activities

3.1.1.1 Truth in Caller ID Act of 2009

The Truth in Caller ID Act of 2009 [6] prohibited the knowing transmittal of "misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value." According to the FCC, caller identity spoofing occurs "when a caller deliberately falsifies the information transmitted to your caller ID display to disguise their identity." This can lead to a caller ID display showing a phone number different from the one from which the call was placed. The Act defines caller identification information as "information provided by a caller identification service regarding the telephone number of, or other information regarding the origination of, a call made using a telecommunications service or IP-enabled voice service." In 2019, the FCC issued Truth in Caller ID Rules [7] which expanded the definition of caller identification information to include text services as well as voice services.

The Truth in Caller ID Act does include some exceptions, including authorized activity of a law enforcement agency or calls from domestic violence shelters. In addition, the Act allows callers to preserve their anonymity by choosing to block all outgoing caller identity information on their phone lines. Some caller identity spoofing is used for legitimate business applications (e.g., to deliver a business telephone number for purposes of call-back, and to protect the caller's privacy if they do not wish to reveal personal telephone numbers used in placing business calls). For example, a doctor calling a patient from his or her personal mobile device may have the office number displayed instead. This legitimate use case for caller identity spoofing may indeed be helpful, not harmful, to the consumer. However, spoofed calls are illegal if the intent is to commit fraud.

3.1.1.2 Declaratory Ruling and Third Further Notice of Proposed Rulemaking In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls and Call Authentication Trust Anchor

In their Declaratory Ruling and Third Further Notice of Proposed Rulemaking In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls and Call Authentication Trust Anchor [4] adopted on June 6, 2019, the FCC noted that the volume of illegal calls is reducing the value of telephony for anyone who makes or receives calls. The FCC further noted that illegal calls can pose a risk to public safety by tying up emergency lines when the calls are made to public safety entities. As a result, the FCC ruled that voice service providers may immediately start offering call-blocking services by default, while giving consumers the choice to opt out, and encouraged voice service providers to implement the SHAKEN caller identity authentication framework. The FCC also proposed a safe harbor for call-blocking programs targeting unauthenticated calls, which may be potentially spoofed, as well as safeguards for critical calls. The FCC further proposed to require that major voice service providers implement SHAKEN if they did not do so on their own by the end of 2019.

In their Ruling [4], the FCC reaffirmed their commitment to safeguarding calls from emergency numbers, including calls from "public safety entities, including PSAPs, emergency operations centers, or law enforcement agencies." They further emphasized that voice service providers should make all feasible efforts to ensure that any call blocking tools would avoid blocking emergency calls.

In the associated Third Further Notice of Proposed Rulemaking [4], the FCC took additional steps to protect consumers from illegal calls and ensure the effectiveness and integrity of the SHAKEN caller identity authentication framework by proposing rules to allow voice service providers to block calls based on Caller ID authentication in certain instances. The FNPRM also proposed protections to ensure that important calls are not blocked (e.g., calls to/from emergency services, calls from alarm companies, calls from local governments or schools). Furthermore, they proposed to require that voice service providers support the SHAKEN caller identity authentication framework, if the major voice service providers had not so by the end of 2019.

At the request of industry stakeholders, the FCC, in their Third Further Notice of Proposed Rulemaking [4], proposed a safe harbor for voice service providers that choose to block calls (or a subset of calls) that fail caller identity authentication under the SHAKEN framework. The FCC noted that call-blocking programs that consider the attestation level associated with the caller identity information (see Section 4 for further details) for successfully authenticated calls would not fit within the scope of this safe harbor. Only calls for which attestation information is available and which fail authentication would be blocked.

In addition, in their Third Notice of Proposed Rulemaking [4], the FCC indicated that certain types of emergency calls must never be blocked. In support of that requirement, the FCC considered requiring any voice service provider that offers call-blocking to maintain a "Critical Calls List" of numbers it may not block. This list would include the outbound numbers associated with PSAPs, as well as government emergency outbound numbers. They further suggested that the prohibition on call blocking would only apply to authenticated calls. Through the Third Notice of Proposed Rulemaking the FCC sought comment from the industry on this proposal. The FCC also discussed potential risks associated with the use of centralized lists of acceptable calling numbers, particularly if illegal callers were able to get access to them, and used that as a justification for limiting lists to "genuine emergency calls only." By limiting call blocking prohibition to calls that are signed and pass authentication, the FCC felt that illegal robocallers would be prevented from spoofing a number on the Critical Calls List since the caller could be more easily identified and the delivery of calls from public safety/government agencies to American consumers would be better assured.

The FCC emphasized that voice service providers should not block emergency calls and reiterated that the Commission's rules prohibit voice service providers from blocking emergency calls to 9-1-1. However, they did raise questions regarding the extent to which PSAPs receive calls where the caller identity is spoofed and a false emergency is reported, and whether there are mechanisms that would enable blocking of illegal spoofed calls to PSAPs without blocking legitimate 9-1-1 calls.

Among the other topics addressed in the Third Notice of Proposed Rulemaking, the FCC noted that SHAKEN, as currently specified, is intended for IP-based networks, and therefore does not address calls that originate in, terminate to, or transit Time Division Multiplexing (TDM) networks. They questioned whether there are technologies available to enable legacy networks to participate in caller identity authentication and sought feedback on what steps could be taken to promote or require caller identity authentication in legacy networks.

3.1.1.3 Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act

The TRACED Act [8] provides tools to discourage illegal robocalls, protect consumers, and crack down on offenders. It expands the window in which the FCC can pursue intentional scammers and levy fines from 1 year to 4 years. The legislation also requires telephone service providers to adopt call verification technologies that would help prevent illegal robocalls from reaching consumers. The TRACED Act [8] recognizes the importance of legitimate calls and ensures important calls like emergency public safety calls are not wrongly blocked. The TRACED Act [8] also addresses the issue of "one-ring scams," where typically international scammers try to get individuals to return their calls so they can charge them exorbitant fees. In addition, it directs the FCC to convene a working group to address the problem of illegal robocalls being made to hospitals.

The TRACED Act [8], which was signed into law in December 2019, addresses the following three topics with respect to robocalling mitigation: (1) authentication; (2) blocking; and (3) enforcement. It requires carriers to adopt call authentication technologies so they can verify that incoming calls are legitimate before they reach consumers' phones. Specifically, the Act [8] specifies that, not more than 18 months after its adoption, the FCC shall require voice service providers that support IP-capable networks to adopt and fully deploy the SHAKEN authentication framework The FCC must also require voice service providers that operate non-IP networks to take reasonable measures to implement an effective call authentication framework. In addition, providers of voice services are prohibited from adding any additional line item charges to consumer or small business customer subscribers to support the implementation of effective call authentication technology.

The Act [8] also places the following additional requirements on the FCC. Specifically, it requires that, within 12 months of the date of enactment, the FCC issue best practices that providers of voice service may use as part of the implementation of effective call authentication frameworks to ensure that the calling party is accurately identified. The Act [8] further provides for the FCC to require voice service providers to block unverified calls at no charge to consumers. It requires that no later than 1 year after its enactment, the FCC shall define rules that specify when a provider of voice service may block a voice call based, in whole or in part, on information provided by a call authentication framework, with no additional line item charge. Within this timeframe the FCC is also required to establish a safe harbor for voice service providers to protect them from liability for unintended or inadvertent blocking of calls or for the unintended or inadvertent misidentification of the level of trust for individual calls based, in whole or in part, on information provided by a call authentication framework. In addition, the Act [8] notes that the rules adopted by the FCC shall make all reasonable efforts to avoid blocking emergency public safety calls.

3.1.1.4 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

This Report and Order and Further Notice of Proposed Rulemaking [5], adopted and released on March 31, 2020, is one of several steps the FCC is taking to implement the TRACED Act [8] described above.

In this Report and Order [5], the FCC adopted the proposal it made in the 2019 Further Notice to require voice service providers to implement the SHAKEN framework. Specifically, the FCC requires all originating and terminating voice service providers to fully implement SHAKEN on the portions of their voice networks that support the transmission of SIP calls, and to exchange calls with authenticated caller ID information with interconnected providers. Thus, through its Report and Order [5], the FCC adopted the following three requirements:

(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 FCC limited application of the rules it adopted through the Report and Order to only the IP portions of voice service providers' networks (i.e., those portions that are able to initiate, maintain, and terminate SIP calls).

In the Report and Order [5], the FCC set an implementation deadline of June 30, 2021 for voice service providers to implement the SHAKEN caller identity authentication framework in the IP portions of their networks. There were two drivers for the FCC setting the deadline when they did. First, to meet the requirements of the TRACED Act [8], the FCC needed to set a deadline for implementation of SHAKEN that would not be more than 18 months after enactment of the Act. Second, they viewed this deadline as providing sufficient time for the FCC to implement, and for voice service providers to gain, a meaningful benefit from implementation of the exemption and extension mechanisms established by the TRACED Act [8].

The FCC declined to require voice service providers to display SHAKEN verification results to their subscribers or to mandate the use of any particular specifications in determining what should be displayed. Rather, the FCC encouraged voice service providers to find the solutions that work best for their subscribers.

One of the proposals made in their Further Notice of Proposed Rulemaking was to extend the FCC's SHAKEN mandate to intermediate providers. Specifically, the FCC proposed that intermediate providers would be required to pass any Identity header they receive, unchanged, to any subsequent intermediate or terminating voice service provider in the call path. The FCC anticipated that imposing such a mandate on intermediate providers would be necessary to ensure that IP calls retain authentication information across the entire call path.

As discussed in Section 3.1.1.3, the TRACED Act [8] also included provisions for support of caller identity authentication in non-IP networks. In their Further Notice of Proposed Rulemaking [5], the FCC notes that, based on the provisions of the TRACED Act [8], the FCC must, by no later than June 30, 2021, require voice service providers to take "reasonable measures" to implement an effective caller ID authentication framework in the non-IP portions of their networks. The FCC interpreted "reasonable measures" as being where the voice service provider is actively working to implement a caller identity authentication framework on the non-IP portions of its network, either by upgrading those portions to IP so that the STIR/SHAKEN authentication framework may be implemented, or by working to develop a non-IP authentication solution by participating in a working group or consortium that is working to develop a non-IP solution, or actively testing such a solution. The approach being taken by the FCC seems to be one of promoting the transition to IP while simultaneously encouraging voice service providers to develop a non-IP solution that may benefit those legacy networks that are not yet in transition.

3.1.1.5 Second Report and Order In the Matter of Call Authentication Trust Anchor

This Report and Order [9], adopted and released on October 1, 2020, reflects further steps taken by the FCC to implement the TRACED Act [8] described above. As described in Section 3.1.1.4, in their first Caller ID Authentication Report and Order and FNPRM [5], the FCC proposed criteria for meeting the "reasonable measures" requirement under section 4(b)(1)(B) of the TRACED Act [8] with regard to supporting call authentication in the non-IP portions of voice service provider networks. In their Second Report and Order [9], they adopted a new rule reflecting this proposal and clarified its specific requirements. Unless granted an extension (as described below), the Second Report and Order [9] requires that, by June 30, 2021, a voice service provider either upgrade its entire network to allow for the initiation, maintenance, and termination of SIP calls and fully implement SHAKEN throughout its network, or "maintain and be ready to provide the Commission on request with documented proof that it is participating, either on its own or through a representative, including third party representatives, as a member of a working group, industry standards group, or consortium that is working to develop a non-Internet Protocol caller identification authentication solution, or actively testing such a solution."

The Second Report and Order [9] does allow for the following extensions with regard to meeting the above requirements: "(1) a two-year extension to small, including small rural, voice service providers; (2) an extension to voice service providers that cannot obtain a certificate due to the Governance Authority's token access policy until such provider is able to obtain a certificate; (3) a one-year extension to services scheduled for section 214 discontinuance; and (4) as required by the TRACED Act [8], an extension for the parts of a voice service provider's network that rely on technology that cannot initiate, maintain, and terminate SIP calls until a solution for such calls is readily available."

In addition, the Second Report and Order [9] requires that intermediate voice service providers implement SHAKEN in the IP portions of their networks no later than June 30, 2021. Specifically, an intermediate provider is required to pass, unaltered, any authenticated caller identification information it receives with a SIP call, unless doing so will result in a failure to complete the call or where such information is believed to cause an imminent threat to its network security. Intermediate service providers will also be required to authenticate caller identification information for all calls it receives for which the caller identification information has not been authenticated and which it will exchange with another provider as a SIP call, unless it registers with the industry traceback consortium or "it responds fully and in a timely manner to all traceback requests it receives from the Commission, law enforcement, and the industry traceback consortium regarding calls for which it acts as an intermediate provider."

Finally, voice service providers are prohibited from adding any additional line item charges to consumer or small business customer subscribers for implementing the required call authentication technology.

3.1.1.6 Sixth Report and Order In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls, Fifth Report and Order In the Matter of Call Authentication Trust Anchor

Foreign-originated calls are a significant portion, if not the majority, of illegal robocalls. Many providers facilitating illegal robocalls are gateway providers[1] and the upstream foreign originating and intermediate providers from whom they receive foreign-originated calls. As a result, gateway providers serve as a critical choke-point for reducing the number of illegal robocalls received by American consumers. A gateway provider may not know the identity or location of the entity that originated the call, but it will know the identity of the immediate upstream provider that sent the call to the gateway provider, including whether that provider has registered as a foreign provider in the Robocall Mitigation Database. The FCC and Congress have long acknowledged that illegal robocalls that originate abroad are a significant part of the robocall problem. Congress highlighted this problem in 2018 when it passed the RAY BAUM'S Act, which prohibits spoofing calls or texts originating outside the U.S.

In the Gateway Provider Report and Order, Order on Reconsideration, Order, and Further Notice of Proposed Rulemaking, released May 20, 2022 [23], the FCC requires that, by June 20, 2023, gateway providers apply STIR/SHAKEN caller ID authentication in the IP portions of their networks to all unauthenticated foreign-originated SIP calls that have U.S. North American Numbering Plan (NANP) calling numbers.[2] Gateway providers have the flexibility in implementing call authentication to assign the level of attestation appropriate to the call based on the call information available to the gateway provider; gateway providers are not limited to assigning "gateway" (C-level) attestation to the call. In addition, gateway providers are required to file with the Robocall Mitigation Database, submitting information that certifies to the status of STIR/SHAKEN implementation and robocall mitigation on their networks; submits contact information for a person responsible for addressing robocall mitigation-related issues; and describes in detail their robocall mitigation practices. Under this rule, downstream providers are prohibited from accepting

[1] The FCC defines a "gateway provider" as a U.S.-based intermediate provider that receives a call directly from a foreign originating provider or foreign intermediate provider at its U.S.-based facilities before transmitting the call downstream to another U.S.-based provider.

[2] Specifically, not later than June 30, 2023, a gateway provider shall either (i) Upgrade its entire network to allow for the processing and carrying of SIP calls and fully implement the STIR/SHAKEN framework throughout its network; or
(ii) maintain and be ready to provide the Commission on request documented proof that it is participating, either on its own or through a representative, including third party representatives, as a member of a working group, industry standards group, or consortium that is working to develop a non-internet Protocol caller identification authentication solution, or actively testing such a solution.

any traffic from a gateway provider that is not listed in the Robocall Mitigation Database. The Order further clarifies that emergency calls to 9-1-1 from originating providers not in the Robocall Mitigation database must not be blocked under any circumstances. In addition, gateway providers must make all reasonable efforts to ensure that calls from PSAPs and government emergency numbers are not blocked.

3.1.2 Regulatory Activities in Canada

In Canada, the Canadian Radio-television and Telecommunications Commission (CRTC) shares many of the same concerns as the FCC with regards to the issues of Robocalling and caller identity spoofing. Accordingly, a number of directives from the Commission have been given to Telephony Service Providers in Canada which include:

- Measures to reduce caller identification spoofing and to determine the origins of nuisance calls, Compliance and Enforcement and Telecom Decision CRTC 2018-32 (https://crtc.gc.ca/eng/archive/2018/2018-32.htm), as amended.
- Implementation of universal network-level blocking of calls with blatantly illegitimate caller identification, Compliance and Enforcement and Telecom Regulatory Policy CRTC 2018-484 (https://crtc.gc.ca/eng/archive/2018/2018-484.htm), as amended.
- Status of implementation by telecommunications service providers of authentication/verification measures for caller identification, Compliance and Enforcement and Telecom Decision CRTC 2019-402 (https://crtc.gc.ca/eng/archive/2019/2019-402.htm), as amended.
- Establishment of the Canadian Secure Token Governance Authority, Compliance and Enforcement and Telecom Decision CRTC 2019-403 (https://crtc.gc.ca/eng/archive/2019/2019-403.htm).
- STIR/SHAKEN implementation for Internet Protocol-based voice calls Compliance and Enforcement and Telecom Decision CRTC 2021-123 (https://crtc.gc.ca/eng/archive/2021/2021-123.htm).

In the most recent decision, the CRTC laid out a mandate for Telecommunications Service Providers (TSPs) to comply with the implementation and reporting requirements for STIR/SHAKEN with the caveat that the decision applies only to IP-based calling (the CRTC did not direct that STIR/SHAKEN capabilities be implemented for legacy TDM calling).

In addition, the CRTC Interconnection Steering Committee (CISC) Network Working Group (NTWG) has a number of working groups looking into various technological aspects related to Robocalling and caller identity spoofing.

- Working group TIF 37 dealt with tracking TSP implementation of STIR/SHAKEN and it filed its fourth and final report in March of 2021 and is no longer active. (https://crtc.gc.ca/public/cisc/nt/NTRE071_TIF%2037.pdf).
- Working group TIF 38 is tasked with measures to determine the origins of nuisance calls (including traceback). This group continues to meet to discuss traceback-related activities. The group produced its final quarterly report August of 2022 (https://crtc.gc.ca/public/cisc/nt/NTRE078.pdf).
- Working group TIF 40 is tasked with the development of a framework for STIR/SHAKEN in Canada. This group has published a document outlining "best practices" for STIR/SHAKEN in Canada and continues to meet as necessary to keep the document up to date (https://crtc.gc.ca/public/cisc/nt/NTGLSTSH20.docx).

Finally, the Chair of the CRTC Emergency Services Working Group (ESWG) filed a letter with the CRTC in relation to Emergency Calling and Emergency Callback Considerations for STIR/SHAKEN Implementations advising that annual updates are to be filed to best align the introduction of STIR/SHAKEN into the Next-Generation 9-1-1 deployment currently underway in Canada (https://crtc.gc.ca/public/cisc/es/ESRE0101.pdf).

4 Overview of SHAKEN Call Identity Authentication and Verification Mechanism

The SHAKEN caller identity authentication and verification processes rely on the transmission of cryptographically signed information to attest to the accuracy of caller identity information transmitted with a call. The SHAKEN framework relies on the originating voice service provider attesting to the caller's identity, and the terminating voice service provider verifying the identity of the originator of the message that contains the caller identity. The SHAKEN architecture calls for the originating service provider to use X.509 [10]-based certificates to "sign" the call information. At the terminating end, a process of verifying that signature helps assess the level of trust in the call information provided by the originating service provider. This 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.[3] Thus, the SHAKEN model calls for the originating service provider to sign the call information (authentication service) with the appropriate private key, and for the terminating service provider to verify the signing credentials (verification service). It is

[3] See ATIS-1000080 [22][22], *Signature-based Handling of Asserted information using toKENs (SHAKEN): Governance Model and Certificate Management*, for details related to SHAKEN governance and certificate management.

important to emphasize that the verification confirms the identity of the signer of the received content before displaying the caller identity to its customers; *it does not specifically verify the caller identity itself*.

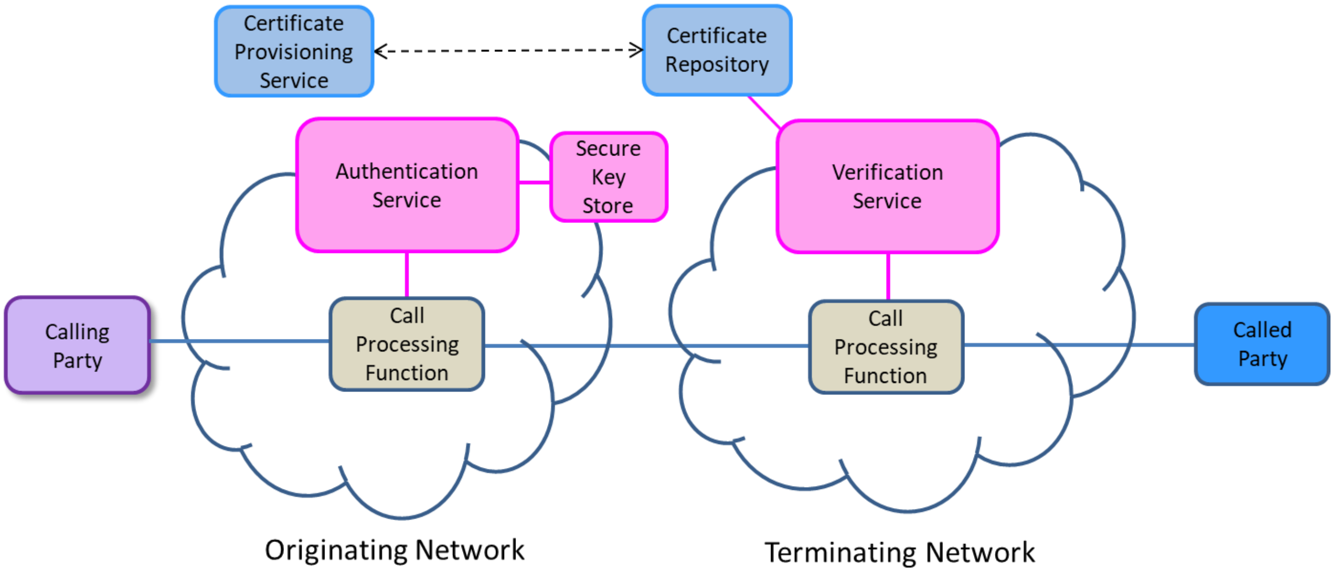


Figure 4-1 High-Level SHAKEN Architecture

SHAKEN uses an assigned attestation indicator, and a unique origination identifier identifying how and where the call originated in the Voice over Internet Protocol (VoIP) network, to represent the ability for the originating network provider that signed the call information 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 that the service provider may have received from an unauthenticated network or that are unsigned.

The SHAKEN framework, as specified in ATIS-1000074 [11] defines three levels of attestation:

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

In asserting an attestation level of "A", the signing provider is indicating 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 ascertained that the customer is authorized to use a number (e.g., by business agreement or evidence that the customer is allowed access to the 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 "legitimate right to assert a telephone number," recognizing that the service provider's reputation may be impacted by how rigorous they have been in making this assertion.

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.

When 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. Gateway attestation may also be used when there is not sufficient information for determining that "A" or "B" attestation applies, even when the call was received via a customer interface.

It is important to emphasize that the SHAKEN framework is only applicable to IP-based service provider voice networks (also to be referred to as VoIP networks). It relies on transmission of information via Session Initiation Protocol (SIP) messages and therefore can only operate on the 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. For that reason, the TRACED Act [8] described in Section 3.1.1.3 and the FCC Report and Order described in Section 3.1.1.4 only require the implementation of SHAKEN on the IP portions of voice service provider networks. Since SHAKEN is a SIP-based solution, those portions of a voice service provider's network that are not capable of initiating, maintaining, and terminating SIP calls cannot authenticate or verify calls under that framework. As noted in Section 3.1.1.3, the TRACED Act [8] contains provisions that require voice service providers to take "reasonable measures" to implement an effective caller ID authentication framework in the non-IP portions of their networks. In the FNPRM described in Section 3.1.1.4, the FCC interprets that provision of the TRACED Act [8] 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 have identified alternative solutions for caller authentication for non-IP traffic. This work has addressed scenarios where SIP connectivity is not available end-to-end and has identified mechanisms for determining whether the calling user is authorized to use a particular calling telephone number.

It is Important to understand that SHAKEN was designed to provide a secure mechanism for the originating carrier to communicate its attestation of the calling telephone number to the terminating carrier; nothing more. A verified telephone number does not mean that the caller identity has not been spoofed or that the call intent is benign.

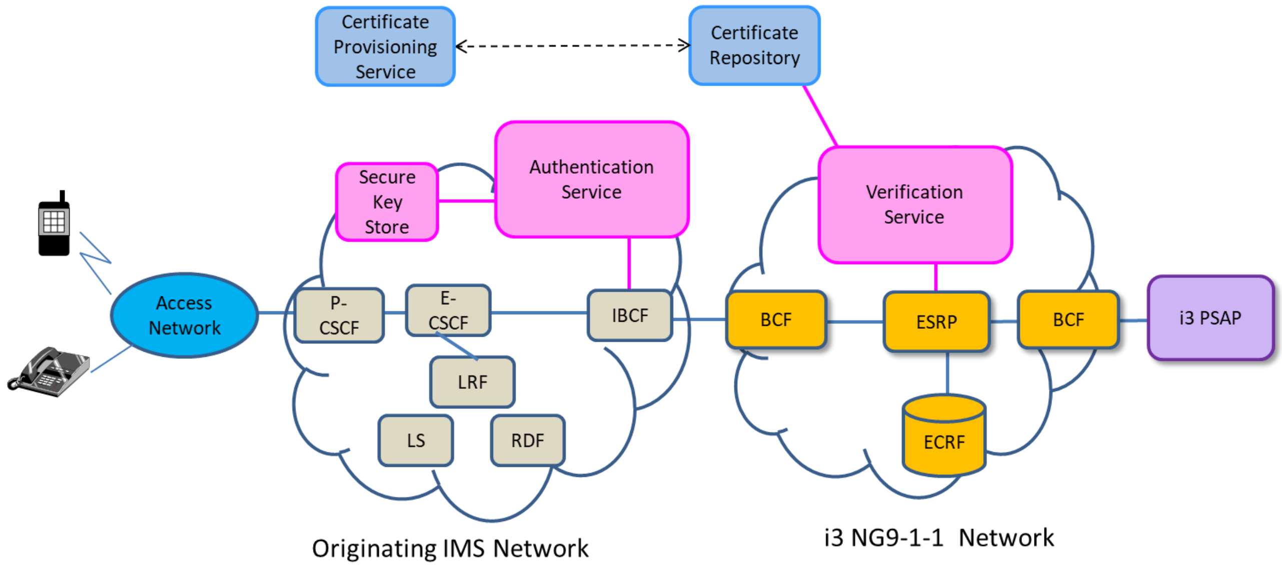
5 Application of SHAKEN Spoofing Mitigation Techniques to Emergency Calling

Caller identity spoofing may disrupt the delivery of emergency services in life-or-death situations. Enabling voice service providers to more effectively identify spoofed calls to emergency services should benefit public safety by reducing the risk of such situations. While the initial standards related to SHAKEN developed by ATIS and elsewhere (e.g., IETF and the 3rd Generation Partnership Project [3GPP]) addressed mechanisms for caller authentication in general, they did not specifically consider caller authentication in the context of 9-1-1 calls or emergency callbacks. More recently, standards development activities within ATIS, IETF, and 3GPP have addressed the application of SHAKEN caller identity authentication and RPH signing to 9-1-1 and emergency callbacks. In addition, the NENA i3 Standards for Next Generation 9-1-1 Version 3, NENA-STA-010.3-2021 [12], includes procedures that address the application of SHAKEN caller identity authentication/verification procedures to 9-1-1 calls and emergency callbacks in an i3 NG9-1-1 Emergency Services Network.

In applying spoofing mitigation techniques, like SHAKEN, to emergency calling, the unique signaling characteristics and network architectures that are involved in supporting 9-1-1 originations and emergency callbacks have required some extensions to the base SHAKEN framework. For example, SIP signaling associated with a 9-1-1 call includes an emergency service Uniform Resource Name (URN) (i.e., a service URN in the "sos" family) in an element that is used in identifying the destination for the call. The original SHAKEN framework assumed that destination information will always be in the form of a telephone number. Extensions were needed to the caller identity authentication and verification procedures to allow destination information (i.e., a "dest" claim) to be in the form of a service URN in the 'sos' family. Also, as discussed in Section 3, unlike non-emergency calls, the signaling associated with a 9-1-1 call and an emergency callback include an RPH. The SHAKEN framework has also been extended to support procedures to sign and verify the RPH to address concerns related to the spoofing of this information. Further extensions were also developed to support the signing and verification of the SIP Priority header, which is used to mark emergency callbacks, to mitigate spoofing of this information as well.

The application of the SHAKEN framework to 9-1-1 calls and emergency callbacks was also impacted by the unique characteristics of the network architectures used to support 9-1-1 calling and emergency callbacks. Elements like the Emergency Call Session Control Function (E-CSCF) in an IP Multimedia Subsystem (IMS) originating network (or IMS-based NG9-1-1 Emergency Services Network) are specific to the processing of 9-1-1 calls. Restrictions surrounding the standard interfaces supported by the E-CSCF required the use of an Hypertext Transfer Protocol (HTTP)-based interface between an Interconnection Border Control Function (IBCF) and an Authentication Service, rather than the SIP interface used between a Call Session Control Function (CSCF) and the Authentication Service, as illustrated in the SHAKEN framework architecture. If the 9-1-1 call is routed via an i3 Emergency Services IP Network (ESInet)/NG9-1-1 Core Services (NGCS), the Emergency Service Routing Proxy (ESRP) will be responsible for interacting with the Verification Service prior to performing routing determination for the call. The ESRP will also be responsible for passing SHAKEN related information (e.g., the results of the verification process) toward the i3 PSAP in a SIP INVITE message.

A high level diagram Illustrating the interconnection of an IMS originating network and an i3 NG9-1-1 network (i.e., ESInet and associated NGCS) in support of 9-1-1 calling is provided below.



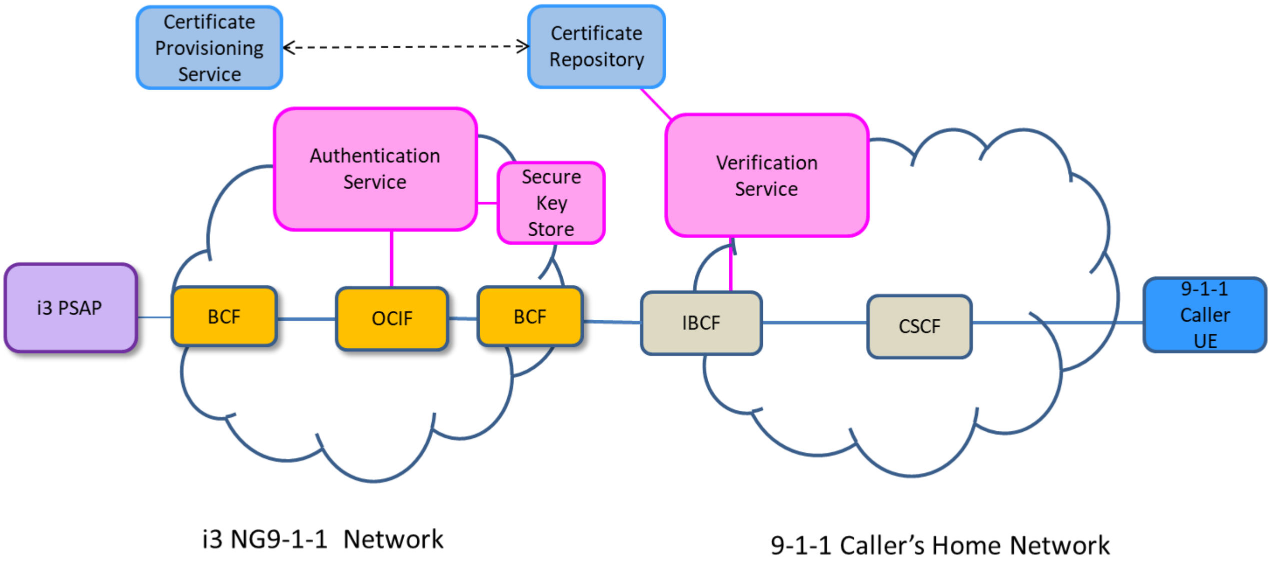
BCF – Border Control Function
ECRF – Emergency Call Routing Function
E-CSCF – Emergency Call Session Control Function
ESRP – Emergency Service Routing Proxy
IBCF – Interconnection Border Control Function

LRF – Location Retrieval Function
LS – Location Server
P-CSCF – Proxy Call Session Control Function
RDF – Routing Determination Function

Figure 5-1 9-1-1 Origination: IMS Originating Network to i3 NG9 1 1 Emergency Services Network

The application of SHAKEN caller identity authentication/verification to 9-1-1 calls must address the handling of 9-1-1 originations where the calling identity is in the form of a non-dialable callback number. There are 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 [13] 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 Emergency Call Session Control Function (E-CSCF) will be responsible for inserting a non-dialable callback number, formatted as described in J-STD-036-C-2 [13], into the SIP signaling associated with the call. If the IMS originating network determines that the emergency call is to be routed to an i3 NG9-1-1 network (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 BCF on the ingress side of the i3 ESInet. As described above, current procedures for applying caller identity authentication to 9-1-1 calls specify that, 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. Based on industry agreements, these procedures will also apply when the caller identity associated with the 9-1-1 call consists of a non-dialable callback number of the form specified in J-STD-036-C-2 [13]. 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 based on ATIS-1000074 [11], an attestation level of "A" should be associated with the non-dialable callback number.

Multiple architectures are possible to support the application of SHAKEN procedures to emergency callbacks, depending on whether the NG9-1-1 Emergency Services Network uses an i3 architecture or an IMS-based architecture, and the architecture used by the 9-1-1 caller's home network. For emergency callbacks routed via an i3 ESInet/NGCS, an Outbound Call Interface Function (OCIF) in the i3 ESInet, if configured through operator policies, is responsible for invoking caller identity authentication and RPH signing by passing the SIP INVITE message associated with the emergency callback to the Authentication Service. The OCIF will invoke the Authentication Service for emergency callbacks after call processing has completed, that is, after the target interconnected network has been determined to be an IP network. The OCIF will include the results of the authentication process (i.e., in the form of Identity headers) in the SIP INVITE message it passes to the interconnected IP network. When the emergency callback reaches the 9-1-1 caller's home network, the Verification Service will be invoked. Depending on the architecture supported by the home network, the Verification Service may be invoked by a Call Processing Function (e.g., an IMS Call Session Control Function) using a SIP interface or by an entry Border Control Function (e.g., an IMS IBCF) using an HTTP interface. The marking of the call as a "psap-callback" using the Priority header can influence how the call is processed in the 9-1-1 caller's home network. For example, the home network may use the fact that it can identify the call as an emergency callback to bypass certain features (e.g., Do Not Disturb) that might normally preclude the call from completing to the 9-1-1 caller. Figure 5-2 illustrates an architecture where an emergency callback is routed via an i3 ESInet/NGCS to an interconnected IMS-based home network that supports invocation of the Verification Service via an IBCF.



BCF – Border Control Function
CSCF – Call Session Control Function
IBCF – Interconnection Border Control Function
OCIF – Outbound Call Interface Function

Figure 5-2 Emergency Callback Routed Via i3 NG9-1-1 Emergency Services Network to IMS Home Network

5.1 Use Cases

This section describes a set of use cases for 9-1-1 calls and emergency callbacks calls that include caller identity information and/or Resource-Priority Headers and that are subject to spoofing mitigation techniques (e.g., SHAKEN, Resource-Priority Header signing).

Use Case #1: 9-1-1 Call Origination with Authentication 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 Resource-Priority Header is signed in the originating network, and both caller identity and RPH undergo verification in the ESInet/NGCS. The 9-1-1 call is then delivered to an i3 PSAP.

Actors

Bob is the caller whose User Equipment (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

Step 1. Bob initiates an emergency call and the call request is forwarded to the originating network.

Step 2. The origination network associates a dialable callback number, an appropriate RPH value, and location information with the call.

Step 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.)

Step 4. The originating network performs location-based routing of the 9-1-1 call and determines that the call is to be routed via an i3 ESInet/NGCS.

Step 5. Based on interactions with an Authentication Service, the caller identity and RPH are signed.

Step 6. The originating network routes the call toward the i3 ESInet/NGCS, passing the signed callback number and RPH and location information (by-value or by-reference).

Step 7. The i3 ESInet/NGCS interacts with a Verification Service which performs verification of the signed caller identity and RPH. In this use case, the verification is successful.

Step 8. The i3 ESInet/NGCS applies location and policy-based routing to the 9-1-1 call.

Step 9. The i3 ESInet/NGCS 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).

Step 10. Carol answers the call.

Step 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.

Step 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.

Step 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" 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[4]

Step 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.)

Step 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 in a pre-SHAKEN environment (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[5]

Step 7. The i3 ESInet/NGCS interacts with a Verification Service that performs verification of the signed caller identity and RPH. In this use case, the verification fails.

Step 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" but verification has failed. Handling of this call may be the same as in a pre-SHAKEN environment (where attestation and verification status information are not available).

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

[4] Only the impacted steps are identified. The other steps are the same as in the Normal Flow.

[5] See note 4 above.

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 i3 ESInet/NGCS network. The Resource-Priority Header and Priority header are also signed in the i3 ESInet/NGCS network, and both the PSAP caller identity and the RPH/Priority header 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 who 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 ESInet/NGCS associates an Attestation Level of "A" with the PSAP caller identity; the caller identity and RPH/Priority header are successfully signed and verified; the emergency callback is delivered to the emergency caller's UE with the PSAP calling number and associated verification status.

Step 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 i3 ESInet/NGCS.

Step 2. The i3 PSAP associates a callback number, an appropriate RPH value, and a Priority header value of "psap-callback" with the call. The PSAP signs the calling number, RPH and Priority header using a certificate traceable to the PSAP Credentialing Agency (PCA).

Step 3. The i3 ESInet/NGCS performs destination routing of the callback call (at the OCIF) 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 i3 ESInet/NGCS and the emergency caller's home network.) The OCIF verifies the PSAP calling number, RPH , and Priority header, all of which have been signed using a certificate traceable to the PCA. Upon successful verification, the OCIF associates an attestation level of "A" with the PSAP calling number.

Step 4. Based on interactions with an Authentication Service, the calling identity (PSAP calling number) is signed using a SHAKEN certificate associated with the NGCS provider. The RPH and Priority header are also signed using a SHAKEN certificate associated with the NGCS provider.

Step 5. The i3 ESInet/NGCS routes the call toward Bob's home network, passing the signed callback number and RPH/Priority header.

Step 6. Bob's home network interacts with a Verification Service which performs SHAKEN verification of the signed caller identity and RPH/Priority header. In this use case, the verification is successful.

Step 7. 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.)

Step 8. 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.

Step 9. Bob answers the call, and he and Carol re-initiate their conversation.

Alternate Flow – The PSAP caller identity is delivered to the ESInet/NGCS with a privacy indicator; the ESInet/NGCS associates an Attestation Level of "A" with the PSAP caller identity; the caller identity, RPH, and Priority header 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.

Step 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 i3 ESInet/NGCS.

Step 2. The i3 PSAP associates a callback number, an appropriate RPH value, and a Priority header value of "psap-callback" with the call. The PSAP signs the calling number, RPH and Priority header using a certificate traceable to the PCA.

Step 3. The i3 ESInet/NGCS performs destination routing of the callback call (at the OCIF) 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 i3 ESInet/NGCS and the emergency caller's home network.) The OCIF verifies the PSAP calling number, RPH , and Priority header, all of which have been signed using a certificate traceable to the PCA. Upon successful verification, the OCIF associates an attestation level of "A" with the PSAP calling number.

Step 4. Based on interactions with an Authentication Service, the calling identity (PSAP calling number), the RPH and the Priority header are signed using a SHAKEN certificate associated with the NGCS provider.

Step 5. The i3 ESInet/NGCS routes the call toward Bob's home network, passing the signed callback number and RPH/Priority header.

Step 6. Bob's home network interacts with a Verification Service which performs SHAKEN verification of the signed caller identity and RPH/Priority header. In this use case, the verification is successful.

Step 7. 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.)

Step 8. 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.

Step 9. Bob answers the call, and he and Carol re-initiate their conversation.

5.2 Public Safety Impacts of Applying Information Spoofing Mitigation Techniques to Emergency Calling

Today, in a legacy E9-1-1 environment, PSAPs are exposed to cybersecurity threats and vulnerabilities that are expected to increase in an NG9-1-1 environment. For example, in an IP environment the spoofing of caller identity is easier to accomplish than in a legacy environment. In the circuit-switched network, anyone attempting to spoof the originating Caller ID would require expensive equipment, advanced knowledge of the switching systems and special access to SS7. IP-enabled communications protocols, such as SIP, have unintentionally facilitated the ability to spoof calling party numbers. In essence, Telephone Number (TN) spoofing occurs when a caller inserts/presents a TN in call origination but call attempts made back to that TN will not terminate to the same interface that originated the call. With a VoIP subscription and with open source software, almost any person can spoof TNs with minimal cost. With the advent of VoIP, access to the PSTN via the Internet has also opened the door to cybersecurity threats such as TN spoofing. Bad actors have taken advantage of this capability for illegitimate and fraudulent purposes.

In the context of emergency calling, the spoofing of caller identity information can be used by bad actors in orchestrating Telephony Denial of Service (TDoS) attacks and swatting attacks.[6] For example, a bad actor may orchestrate an attack in which a large number of calls are made to 9-1-1 from the same or nearby locations (to ensure that the calls are routed to the same PSAP). The bad actor may use caller identity spoofing, changing the caller identity on every call, to avoid detection. The objective of the attack is to tie up resources within the PSAP, preventing the handling of legitimate incoming calls and/or the making of outgoing calls. Calls are answered, with the bad actor's location information and callback information displayed on the call taker's CPE until PSAP call-taking queues fill as the number of 9-1-1 originations exceeds the number of available call takers. (Note that the call handling procedures at the PSAP may be complicated further if the bad actor's calls are delivered as "silent" calls.) It is possible that such an attack could result in enough volume to cause a roll-over to an alternate facility.

With the implementation of SHAKEN caller identity authentication/verification, if such an attack was initiated, the originating network would associate an attestation level with the caller identity (i.e., callback number) based on the relationship that the Originating Service Provider (OSP) has with the caller and the ability of the OSP to recognize whether the caller identity is appropriate for that caller. The bad actor's attempts to use spoofed calling numbers would likely result in the association of an attestation level of "C" with the call, indicating that the OSP does not recognize the caller or the call identity. Based on interactions with an Authentication Service, the caller identity (with the "C" level attestation) would be signed and the call would be signaled forward to the i3 ESInet/NGCS, where verification of the signed caller identity would be performed. Ultimately, the call would be delivered to an i3 PSAP with the caller identity and associated attestation information and verification status. While queues at the PSAP would begin to fill, as the number of 9-1-1 originations exceeds the number of available call takers, the call takers may take notice of the large number of 9-1-1 calls being received with "C" level attestation, causing the PSAP to invoke attack mitigation procedures (while handling received calls per Operating Procedures). The PSAP will recover when the attack ceases (at the discretion of the orchestrator of the attack) or as a result of pre-planned mitigation and recovery actions being invoked.

[6] See the Task Force on Optimal PSAP Architecture (TFOPA) Working Group 1 Report on *Optimal Cybersecurity Approach for PSAPs* [14] for detailed descriptions of the Use Cases on which these threat scenario descriptions are based.

In another example, caller identity spoofing could be used in the context of a swatting attack. Swatting is the act of causing the dispatch of an emergency response based on the false report of an ongoing critical incident. This may be facilitated by directly providing false location information along with the call. Location provided to PSAPs associated with calls from fixed devices (e.g., circuit-switched calls from landlines, or VoIP services that only support emergency service calls from stationary devices) is determined from a lookup using the calling telephone number. As a result, for landlines or fixed VoIP, spoofing of caller identity can result in the PSAP incorrectly determining the caller's location. Ideally, a call taker at a PSAP should be able to assess, in real time, the level of trust that can be placed on the information provided with a call. Where real-time assessment is not possible, it is important to be able to determine the source of the call in a post-incident investigation, so as to be able to enable law enforcement to conduct a criminal investigation.

Swatting can be used to distract emergency services to a location that is different from the location of a criminal action. For example, a bad actor orchestrates a swatting attack by initiating a 9-1-1 call with a spoofed caller identity. Location-based routing is used to deliver the call to the PSAP. The call taker answers the call and initiates the dispatch of emergency services to the spoofed location associated with the spoofed caller identity or provided by the bad actor in response to questions asked by the PSAP related to the 9-1-1 call. First responders travel to the false location(s), reducing the resources available to respond to the location where the criminal action is actually taking place. The presence of first responders at the false location(s) may create confusion, resulting in additional calls being generated to 9-1-1. At the same time, 9-1-1 calls may start arriving associated with the actual crime. Due to the decreased availability to handle the actual crime, the PSAP may need to reach out for mutual aid.

If this scenario were to occur in an area where SHAKEN had been implemented, the OSP would associate an attestation level of "C" with the call from a bad actor using a spoofed number (because the OSP does not recognize the caller or the call identity). The OSP would then sign the caller identity and pass the call to the i3 ESInet/NGCS, where verification of the signed caller identity would be performed. The i3 ESInet/NGCS would apply location- and policy-based routing to the call, and would deliver the call to the i3 PSAP with caller identity (and associated attestation and verification status) and location information.

While the "C" attestation level might be sufficient to raise some suspicion on the part of the PSAP call taker who is handling the call, this scenario illustrates the need for a comparable spoofing mitigation mechanism to be applied to the location information associated with the call. While such a mechanism is outside of the scope of the SHAKEN caller identity authentication mechanism, there has been work in the industry to identify a mechanism by which the signing and verification of the location information associated with 9-1-1 calls could identify and mitigate potential compromise of that information. The availability of information spoofing mitigation techniques, and the delivery of associated attestation (of caller identity) and verification information (associated with caller identity, RPH and location information) to the PSAP with emergency calls, could provide a basis for the invocation of pre-planned mitigation and recovery actions associated with swatting attacks.

5.3 Open Issues

While significant progress has been made in defining architectures, procedures, and protocols to support the application of information spoofing mitigation techniques, such as SHAKEN, to emergency and callback calls, one open issue that needs to be addressed is related to the handling of callback calls with private calling (PSAP) TNs.

There are scenarios where a PSAP may want to keep their identity private when initiating a callback call (e.g., domestic violence scenarios). The ability to authenticate/verify the PSAP TN and convey the verification status associated with the caller identity to the called User Equipment (UE), even though the TN itself is not displayed to the called party, may improve the chances that a callback call gets answered. Current standards related to the handling of private calling numbers specify that the SIP signaling identify the caller as “anonymous” by populating the Uniform Resource Identifier (URI) “sip:anonymous@anonymous.invalid” in the From header of the SIP INVITE message. Since the From header does not contain information that is in the form of a TN (which can be expressed as a tel URI), there is currently no standard way to communication verification status information associated with a private calling number. One option being explored is to add a parameter to the “anonymous” sip URI to convey verification status. Note that the anonymity of the caller should not impact the delivery of the RPH and Priority header fields or associated verification status information.

6 Caller Authentication in an E9-1-1 or Transitional NG9-1-1 Environment

Non-IP call authentication solutions being considered by the industry assume that TDM networks support the ability to obtain caller identity attestation level and verification status information either by implementing new functional elements and/or interfaces to support the acquisition of such information, or by using mappings between SIP and SS7 signaling headers/parameters to pass such information with the call. In assessing the applicability of these approaches to 9-1-1 calls, consideration must be given to the unique architecture and signaling characteristics of E9-1-1 and transitional NG9-1-1 environments.

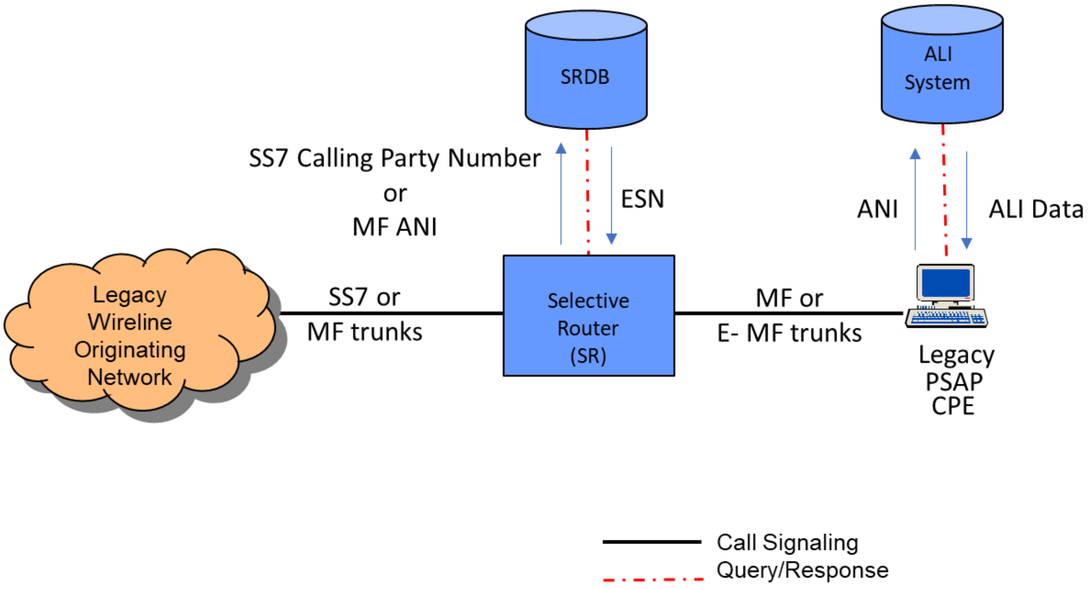
6.1 E9-1-1 Environment

Today, Selective Routers (SRs) typically receive emergency calls over dedicated Multi-Frequency (MF) or Signaling System No. 7 (SS7)-supported trunk groups from wireline end offices and Mobile Switching Centers (MSCs). They use information received in incoming signaling to identify the PSAP that serves the area in which the call originated. SRs deliver the emergency call to the PSAP, typically over traditional Centralized Automated Message Accounting (CAMA)-like (i.e., Traditional MF) or Enhanced Multi-Frequency (Enhanced MF) interfaces. Traditional MF is still in use in certain areas today, and supports the delivery of a 7-digit number, along with a single Numbering Plan Digit (NPD) that can be used to derive the Numbering Plan Area (NPA) and to indicate whether the Automatic Number Identification (ANI) information should be displayed using a steady or flashing display.[7] Enhanced MF is a Feature Group D-like signaling scheme that is more commonly used between SRs and PSAPs. It supports the delivery of either one or two 10-digit numbers to the PSAP with the call, along with an ANI II value that tells the PSAP CPE whether to display the information using a steady or flashing display. The MF signaling stream includes a key that the PSAP will use to query an Automatic Location Identification (ALI) database for the caller's location information. Having retrieved the location information, the PSAP can support the dispatch of emergency personnel to the incident location.

When a wireline caller originates an emergency call, the call is routed from the caller's serving end office, over a (typically dedicated) MF or SS7 trunk group, to an SR. The signaling associated with the 9-1-1 call will include the caller's telephone number signaled as an MF ANI or in an SS7 Calling Party Number parameter. After determining the target PSAP for the call (by querying a Selective Routing Database [SRDB] using the ANI/calling party number), the SR delivers the call along with the telephone number to the PSAP over a Traditional MF or Enhanced MF interface, as appropriate for the PSAP. The delivery of the wireline 9-1-1 caller's telephone number allows PSAPs to access the location information associated with the telephone number by querying the ALI database. In the case of wireline emergency callers, the ALI database contains static telephone number-to-street address mappings. The carrier that serves the PSAP typically operates the ALI databases.

Figure 6-1 shows a representative architecture for wireline E9-1-1.

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



ALI – Automatic Location Identification
ANI – Automatic Number Identification
CPE – Customer Premises Equipment
E-MF – Enhanced Multi-Frequency
ESN – Emergency Service Number

MF – Multi-Frequency
PSAP – Public Safety Answering Point
SR – Selective Router
SRDB – Selective Routing Database
SS7 – Signaling System No. 7

Figure 6-1 E9-1-1 Architecture for Wireline Emergency Calls

In the context of wireless E9-1-1, a Mobile Switching Center (MSC) will provide emergency call-related information to an SR using SS7 or Feature Group-D MF signaling. The interface between the SR and the PSAP may support (depending on PSAP capabilities) the delivery of the two 10-digit numbers (i.e., callback number and a pseudo ANI [pANI]) received from the MSC to the PSAP using the Enhanced MF signaling interface defined by the National Emergency Number Association (NENA). However, there are still PSAPs that support Traditional MF interfaces which, as described above, support the delivery of a 7-digit number and an NPD representing the NPA.

To fulfill wireless E9-1-1 Phase II requirements supporting the delivery of latitude and longitude associated with the 9-1-1 call, wireless carriers have deployed location determination technology in their networks. Due to limitations in today's location determination technology that may result in delays in obtaining Phase II location, existing

Phase II implementations typically support the delivery of Phase I information or a location key in the call setup signaling. Phase II location information is delivered over a separate data link between the wireless network and the emergency services network. The E2 protocol defined in J-STD-036-C-2 [13] and NENA-STA-018.2-2021 (originally NENA 05-001) [16] is typically used over the data link between the wireless network and an ALI system to request/deliver initial caller location information.[8] The ALI system then provides the location information to the PSAP via an ALI interface. The same interfaces can be used to provide updated location information when requested.

J-STD-036-C-2 [13] defines two methods for delivering Phase II location from the wireless network to the emergency services network via a separate data link. One is referred to as the Non-Call Associated Signaling (NCAS) approach, and the other is referred to as the Wireline Compatibility Mode (WCM) approach. Of the two variants, the WCM approach is more widely deployed. With the WCM approach, as defined in J-STD-036-C-2 [13], all the FCC-mandated Phase I and Phase II location information, as well as the callback number, are sent over a separate data link to the ALI database from the wireless network. Call setup signaling between the MSC and the SR includes an Emergency Services Routing Key (ESRK). The ESRK may represent the PSAP or an Emergency Service Zone (ESZ) in the jurisdiction of a PSAP, and also uniquely identifies the 9-1-1 call. In addition, the ESRK uniquely identifies an MPC/GMLC in the wireless network that the ALI system must query to acquire the location information. The ESRK is delivered by the SR to the PSAP over a Traditional MF or Enhanced MF interface with the 9-1-1 call.

Figure 6-2 illustrates wireless emergency call handling using the WCM approach.

[8] There are also some implementations that use the Mobile Location Protocol (MLP) between the ALI system and the Mobile Positioning Center(MPC)/Gateway Mobile Location Center (GMLC) in the wireless network to obtain the location associated with an emergency call.

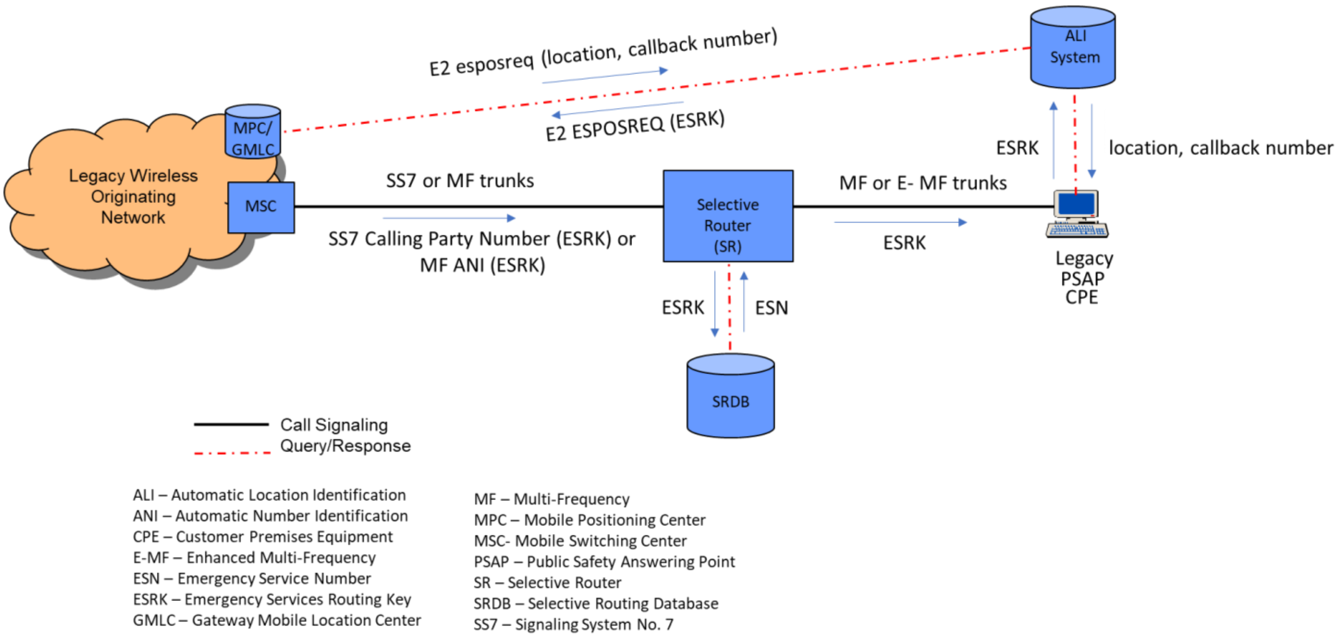

E2 esposreq (location, callback number)
ALI System
MPC/ GMLC
E2 ESPOSREQ (ESRK)
ESRK
location, callback number
Legacy Wireless Originating Network
MSC
SS7 or MF trunks
Selective Router (SR)
MF or E- MF trunks
SS7 Calling Party Number (ESRK) or MF ANI (ESRK)
ESRK
Legacy PSAP CPE
ESRK
ESN
SRDB
Call Signaling
Query/Response
ALI – Automatic Location Identification
ANI – Automatic Number Identification
CPE – Customer Premises Equipment
E-MF – Enhanced Multi-Frequency
ESN – Emergency Service Number
ESRK – Emergency Services Routing Key
GMLC – Gateway Mobile Location Center
MF – Multi-Frequency
MPC – Mobile Positioning Center
MSC- Mobile Switching Center
PSAP – Public Safety Answering Point
SR – Selective Router
SRDB – Selective Routing Database
SS7 – Signaling System No. 7

Figure 6-2 Wireless E9-1-1 – Wireline Compatibility Mode

Industry activities related to caller authentication in non-IP environments have identified two solutions for non-emergency calls. One solution addresses the ability to convey SHAKEN Personal Assertion Tokens (PASSporTs) containing signed caller identity information between networks outside of the call setup signaling. This solution, described in ATIS-1000096, *Signature-based Handling of Asserted information using toKENs (SHAKEN): Out-of-Band PASSporT Transmission Involving TDM Networks* [19], assumes that a TDM originating network supports additional functionality and interfaces to allow for the interworking of SS7 signaling to SIP, the acquisition of a SHAKEN PASSporT, and the publication of that PASSporT to an external system referred to as a Secure Telephone Identity Call Placement Service (STI-CPS). In addition, this solution assumes that a TDM terminating network supports functionality and interfaces that will allow it to perform SS7-IP interworking and retrieve a SHAKEN PASSporT from an STI-CPS.

A second non-IP call authentication solution, documented in ATIS-1000095, *Extending STIR/SHAKEN Over TDM* [20], supports the conveyance of verified attestation levels over TDM interconnections based on bilateral agreements and transitive trust between the operators on each end of a TDM connection. It assumes that SS7 Integrated Services Digital Network User Part (ISUP) signaling is used over the TDM portions of the call path and allows for attestation level and verification status information to be conveyed either using specific values (or spare values) of ISUP parameters (e.g., the ISUP Screening

Indicator in the Calling Party Number parameter) to signal the verified attestation level or by using different trunk groups to convey different attestation level values. ATIS-1000095 [20] describes mappings between Screening Indicator values and attestation level/verification status information. ATIS-1000095 [20] also describes a mechanism by which PASSporT information can be conveyed in an ISUP User to User Information parameter.

Since suppliers of SR equipment are no longer implementing enhancements to those systems, a call authentication solution that requires the SR to support new interfaces is not viewed as technically feasible. Assuming that an SR could obtain attestation level and verification status information associated with a 9-1-1 call based on information received via existing SS7 interfaces (or incoming trunk group), the ability to deliver this information to legacy PSAPs is limited by the MF call delivery interfaces typically supported by legacy PSAPs today. For legacy PSAPs that support Traditional MF interfaces, there does not seem to be an MF signaling-based option for conveying attestation and verification status information with a 9-1-1 call due to the significant signaling limitations associated with such interfaces. Where Enhanced MF interfaces are supported, it might be possible to use spare "II" values to convey attestation and verification status information associated with the caller identity to legacy PSAPs that support Enhanced MF interfaces. This would require the assignment of potentially several more "II" values (to accommodate combinations of attestation level and verification status values), modifications to the call processing supported by SRs to correctly populate the "II" value in the outgoing Enhanced MF signaling based on the attestation and verification status information received in or derived from incoming SS7 signaling (or the incoming trunk group), and correct interpretation of the new "II" values by legacy PSAPs based on new/modified SOPs. Since the use of "II" values to convey attestation level information and verification status to legacy PSAPs that support Enhanced MF interfaces would require modifications to SR call processing, and suppliers of SR systems are no longer supporting upgrades to those systems, non-IP call authentication solutions that use SS7 signaling (or trunk groups) to convey attestation level or verification status information to the SR cannot be viewed as technically feasible.

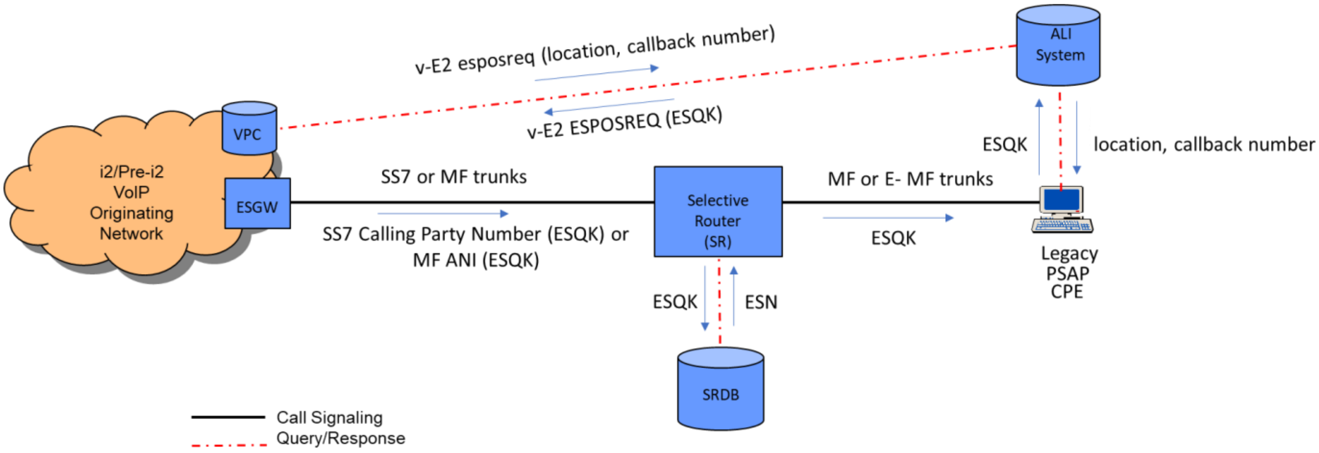
Since delivery of attestation level and verification status information to legacy PSAPs via MF call delivery interfaces is not technically feasible, an alternative is to deliver caller identity attestation level and verification status information to legacy PSAPs via the Automatic Location Identification (ALI) interface. In determining how to effectively use the ALI interface to allow legacy PSAPs to determine the trustworthiness of caller identity information associated with incoming 9-1-1 calls, the following must be considered.

According to ATIS-1000628, *Emergency Calling Service* [21], which describes standards related to E9-1-1 Service, an SS7 Calling Party Number parameter will be populated with a network-provided number (i.e., the Screening Indicator associated with the Calling Party

Number parameter is set to "network provided"), unless (1) the call originates from an ISDN interface, (2) the originating switch allows user-provided numbers from ISDN interfaces to be used as calling party numbers, and (3) the user-provided number passes screening. In the latter (i.e., ISDN) case, the Screening Indicator associated with the Calling Party Number will have the value "user provided, screening passed". Based on ATIS-10000628 [21], a user-provided number that fails screening shall not be sent toward the SR; instead, the main (i.e., network-provided) number shall be sent toward the SR as the calling party number. According to ATIS-1000095 [20], both a Screening Indicator value of "network provided" and a Screening Indicator value of "user provided, screening passed" would be associated with an attestation level of "A" and a verification status ('verstat') value of "TN-Validation-Passed". Since, based on ATIS-1000095 [20], all allowable Screening Indicator parameter values associated with 9-1-1 originations from legacy originating networks will map to an attestation level of "A" and a 'verstat' value of "TN-Validation-Passed", it may be sufficient for a legacy PSAP just to know that the call originated in a legacy wireline or wireless network to associate an "A" attestation level and a 'verstat' of "TN -Validation-Passed" with the information signaled as the calling number. The type of network that the call originated from is known by the SR based on the incoming trunk group, but cannot be determined by the legacy PSAP based on MF signaling associated with a 9-1-1 call. A legacy PSAP can identify 9-1-1 calls that originate in legacy wireline or wireless networks based on the Class of Service (CoS) delivered via the ALI interface (e.g., a CoS value of "Residential" or one of the "Wireless" values). Specifically, CoS values associated with legacy wireline and wireless emergency calls can be used by legacy PSAPs to implicitly associate an attestation level of "A" and verification status of "TN-Validation-Passed" with the callback numbers related to such calls.

6.2 i2/Pre-i2 Architectures

In "i2"/"pre-i2" architectures, an SR will receive 9-1-1 calls that originate in an "i2" or "pre-i2" VoIP network over MF or SS7 trunks from an Emergency Services Gateway (ESGW). The SR will deliver such calls to legacy PSAPs using existing MF or Enhanced MF interfaces. The signaling the SR uses to deliver calls that originate in i2 VoIP networks to legacy PSAPs will look much the same as the signaling used to deliver wireless originations to legacy PSAPs, except that an ESQK will be delivered as the ANI rather than an ESRK. In the context of this architecture, legacy PSAPs receive ALI information from an ALI system that interacts with a VoIP Positioning Center (VPC) using an E2-like interface, similar to the way it would interact with an MPC/GMLC in a wireless originating network. Figure 6-3 illustrates a typical "i2"/"pre-i2" architecture.



ALI – Automatic Location Identification
ANI – Automatic Number Identification
CPE – Customer Premises Equipment
E-MF – Enhanced Multi-Frequency
ESN – Emergency Service Number
ESGW – Emergency Services Gateway
ESQK – Emergency Services Query Key

MF – Multi-Frequency
MSC- Mobile Switching Center
PSAP – Public Safety Answering Point
SR – Selective Router
SRDB – Selective Routing Database
SS7 – Signaling System No. 7
VPC – VoIP Positioning Center

Figure 6-3 i2/Pre-i2 VoIP 9-1-1 Architecture

Callback information associated with 9-1-1 calls that originate in i2/pre-i2 VoIP networks is "network-provided" (i.e., sourced from the VoIP Service Provider's subscription data). Since the mechanism used by the SR to deliver 9-1-1 calls to legacy PSAPs is the same as for calls originating in legacy networks, the same considerations apply with regard to delivering attestation level and verification status information to legacy PSAPs via the call delivery interface for 9-1-1 calls that originate in i2/pre-i2 VoIP networks. In an i2/pre-i2 VoIP environment, consideration should again be given to using the ALI interface to deliver attestation level and verification status information to legacy PSAPs.

As described in Section 3.1.1.4, the Report and Order and Further Notice of Proposed Rulemaking [5], adopted and released on March 31, 2020, requires VoIP Service Providers to implement, by June 30, 2021, authentication of caller identity information associated with outgoing calls exchanged with another voice service provider or intermediate provider, using the STIR/SHAKEN authentication framework. An i2/pre-i2 VoIP Service Provider that has performed SHAKEN authentication on the caller identity provided with a 9-1-1 call could pass the resulting attestation level and verification status information from the VPC to a legacy ALI system, and from a legacy ALI system to a legacy PSAP, using the Customer Name field in the Location Description parameters in the v-E2 and legacy ALI interfaces. (See Section 6.4 for further discussion.) This assumes that i2/pre-i2 VoIP networks have been enhanced to support STIR/SHAKEN and that they will support the real-time updating of the Customer Name field returned by the VPC to indicate the results of the caller identity authentication process.

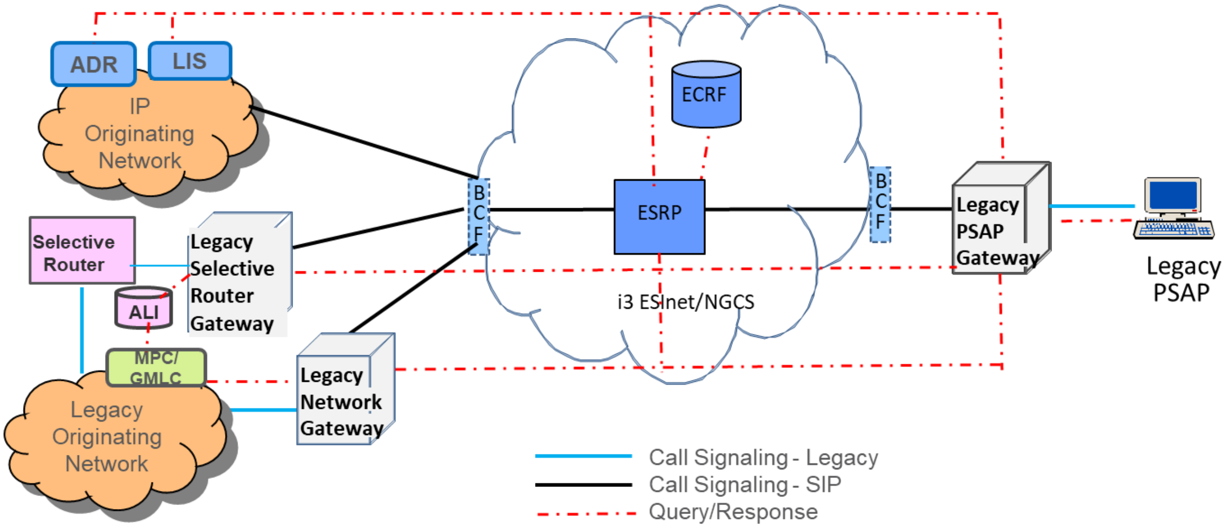
If the i2/pre-i2 VoIP network provider has not yet implemented STIR/SHAKEN or does not support the ability to update in real-time the Customer Name information populated in the VPC with the attestation level and verification status associated with the callback number, the PSAP may receive an explicit indication that the attestation level and verification status associated with the callback information is "unavailable" based on provisioning associated with the Customer Name field provided to it by the VPC via the ALI interface. Unlike 9-1-1 calls originating in legacy networks, there is no consistent association between i2/pre-i2 VoIP originations and the CoS values delivered to legacy PSAPs for those calls. That means that the legacy PSAP cannot determine, based on the CoS, that the call came from an i2/pre-i2 network and that the callback information provided with the call is network-provided. While a variety of CoS values are being used in i2/pre-i2 VoIP 9-1-1 implementations, the ability to successfully retrieve a network-provided callback number based on interactions between an ALI system and a VPC will allow a PSAP to apply appropriate call handling (as specified in SOPs) based on the knowledge that the callback number is network-provided even though it has not received an explicit indication of the specific attestation level and verification status.

6.3 Transitional NG9-1-1 Architectures Involving Legacy PSAPs

NG9-1-1 Emergency Services Networks will be required to support 9-1-1 originations from legacy originating networks and SRs as well as the delivery of emergency calls to legacy PSAPs. As a result, gateway functionality will be a required part of any transitional NG9-1-1 Service Architecture. This section focuses on transitional architectures that involve the delivery of 9-1-1 calls that are routed via an i3 ESInet/NGCS to a legacy PSAP.

6.3.1 Transitional NG9-1-1 Architectures that Include Legacy PSAP Gateways

In one transitional architecture, 9-1-1 calls (and associated data) that are routed via an i3 ESInet/NGCS, are delivered to legacy PSAPs via a Legacy PSAP Gateway (LPG) that serves as the signaling and media interconnection point between the i3 ESInet/NGCS and the legacy PSAP. The SIP signaling delivered to an LPG by an i3 ESInet/NGCS will contain the same information as the SIP signaling that is delivered to an i3 PSAP, including location information (by reference or by value) and callback information. The LPG is responsible for interworking the SIP signaling to the Traditional MF or Enhanced MF signaling that is appropriate for the interface over which the call will be delivered to the legacy PSAP. Location information received by the LPG will be provided to the legacy PSAP outside of the call setup process via a legacy ALI interface. The LPG will look to the legacy PSAP like an ALI system and the legacy PSAP will query the LPG using the same interface as it would use to query an ALI database. Figure 6-4 illustrates a transitional NG9-1-1 architecture that includes an LPG.



ADR– Additional Data Repository
ALI – Automatic Location Identification (System)
BCF – Border Control Function
ECRF – Emergency Call Routing Function
ESInet – Emergency Services IP Network

ESRP – Emergency Service Routing Proxy
GMLC – Gateway Mobile Location Center
LIS – Location Information Server
MPC – Mobile Positioning Center
NGCS – NG9-1-1 Core Services
PSAP – Public Safety Answering

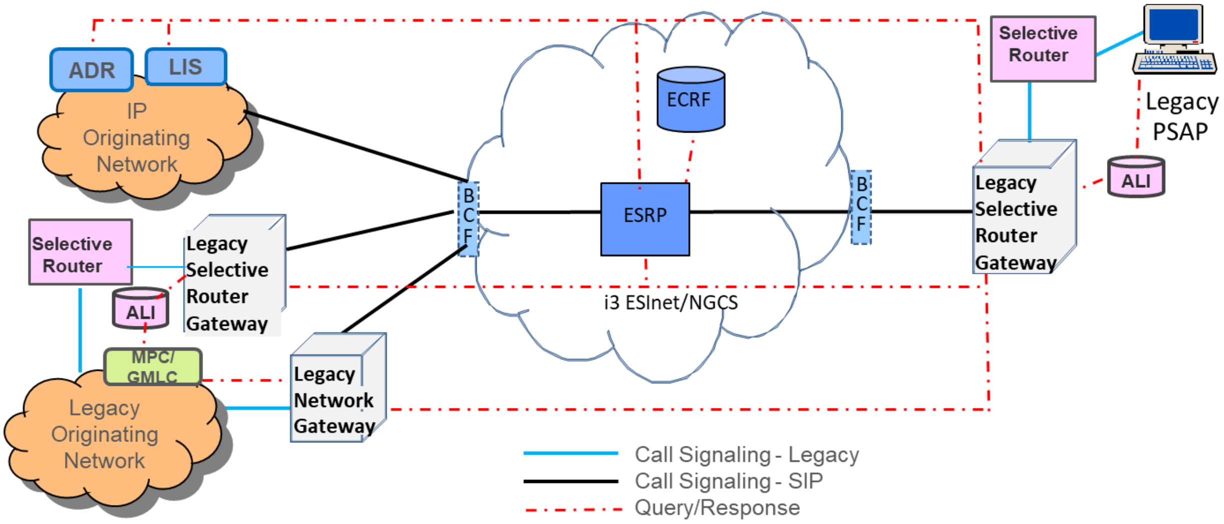
Figure 6-4 Transitional NG9-1-1 Architecture with LPG

Since, by design, an LPG will interface to a legacy PSAP for 9-1-1 call delivery in the same way as an SR does, the same considerations apply to delivering attestation level and verification status information over MF call delivery interfaces using this transitional architecture as for a legacy E9-1-1 architecture. The legacy ALI interface between the LPG and the legacy PSAP is a viable option for delivering attestation level and verification status information to legacy PSAPs associated with 9-1-1 calls that are routed via LPGs.

Since, in transitional architectures involving LPGs, a 9-1-1 call may originate in a legacy or IP/SIP-based originating network, an attestation level of "A", "B", or "C" and a verification status of "TN-Validation-Passed", "TN-Validation-Failed", or "No-TN-Validation" may be received by the LPG in incoming SIP signaling. To accommodate conveyance of all combinations of attestation level and verification status that might be received by an LPG, an analysis was needed to determine which fields in existing ALI interfaces might be candidates for conveying attestation level and verification status to legacy PSAPs in the context of these types of transitional architectures. See Section 6.4 for further details.

6.3.2 Transitional Architectures that include Egress Legacy Selective Router Gateways

An emergency call that is routed via an i3 ESInet/NGCS and is destined for a legacy PSAP that is connected to an SR must traverse a Legacy Selective Router Gateway (LSRG) on the egress side of the ESInet/NGCS. The LSRG delivers the emergency call to the SR over an SS7 supported tandem-to-tandem trunk group. The LSRG will also need to be able to pass a key to the location information received in incoming signaling associated with the emergency call to the SR, either by itself (i.e., populated in the SS7 Calling Party Number parameter) or in addition to the callback information (where the callback information is populated in the SS7 Calling Party Number parameter and the location key is populated in the SS7 Generic Digits Parameter). An egress LSRG must therefore also generate a 10-digit pANI to associate with the location information received in incoming signaling from the i3 ESInet/NGCS. The SR will use the appropriate MF interface to deliver the emergency call to the legacy PSAP. The MF signaling will include the location key/pANI generated by the LSRG to allow the PSAP to query the ALI system, and the ALI system to steer the query to the LSRG as if it were an MPC/GMLC or VPC. The LSRG will be responsible for returning location information, as well as the callback number and other non-location information, in the response to the ALI system, which will then pass it via a legacy ALI interface to the PSAP. See Figure 6-5 for an illustration of this transitional architecture.



ADR– Additional Data Repository
ALI – Automatic Location Identification (System)
BCF – Border Control Function
ECRF – Emergency Call Routing Function
ESInet – Emergency Services IP Network

ESRP – Emergency Service Routing Proxy
GMLC – Gateway Mobile Location Center
LIS – Location Information Server
MPC – Mobile Positioning Center
NGCS – NG9-1-1 Core Services
PSAP – Public Safety Answering

Figure 6-5 Transitional NG9-1-1 Architecture with Egress LSRG

Since, in the context of this transitional architecture, call delivery is from the SR to the PSAP (as it is in an E9-1-1 architecture), the same considerations apply regarding the delivery of attestation level and verification status information to the legacy PSAP via the call delivery interface. Like the transitional NG9-1-1 architecture that includes the LPG, transitional architecture involving egress LSRGs will process 9-1-1 calls that originate in a legacy or IP/SIP-based originating network, and may therefore receive incoming SIP signaling that includes an attestation level of "A", "B", or "C" and a verification status of "TN-Validation-Passed", "TN-Validation-Failed", or "No-TN-Validation". However, to support the delivery of all combinations of attestation level and verification status information over the ALI interface to the legacy PSAP, the LSRG must be able to convey attestation level and verification status information over the E2 (or PSAP to ALI Message [PAM]) interface between itself and the ALI system. To support this transitional architecture, an analysis was needed to determine which fields in existing ALI interfaces and E2 interfaces might be candidates for conveying attestation level and verification status to legacy PSAPs. See Section 6.4 for further information.

6.3.3 Interconnection of IMS Originating Networks and Legacy SRs

Legacy PSAPs may also receive 9-1-1 calls from SRs that interconnect with a Media Gateway Control Function (MGCF)/Media Gateway (MGW) in an IMS originating network. In that case, the 9-1-1 call will be delivered to the SR over an SS7 or MF trunk group, with signaling that includes a pANI created by the IMS originating network. This pANI will be delivered to the legacy PSAP over an existing MF or Enhanced MF interface, and will be used by the legacy PSAP to query the ALI system. The ALI system will use the pANI to interact with a Location Retrieval Function (LRF) in the IMS originating network as if it were an MPC/GMLC. This interconnection architecture is illustrated in Figure 6-6.

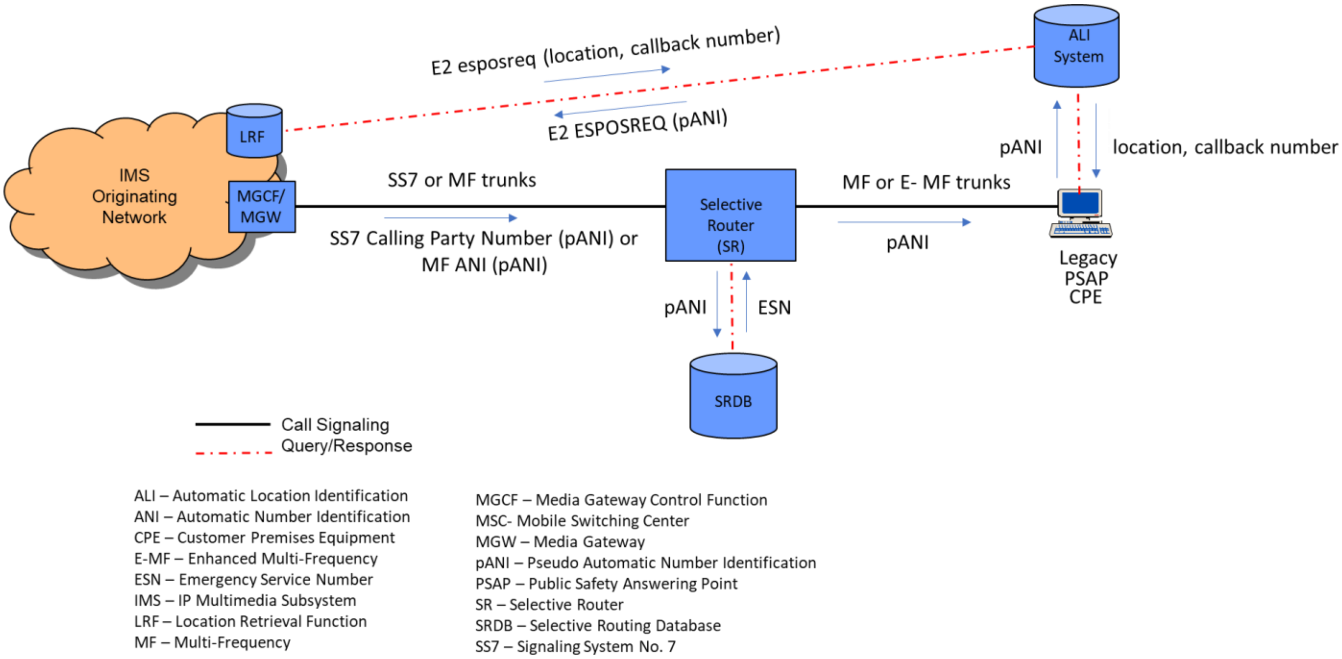

E2 esposreq (location, callback number)
ALI System
E2 ESPOSREQ (pANI)
LRF
pANI
location, callback number
IMS Originating Network
MGCF/ MGW
SS7 or MF trunks
Selective Router (SR)
MF or E- MF trunks
SS7 Calling Party Number (pANI) or MF ANI (pANI)
pANI
Legacy PSAP CPE
pANI
ESN
SRDB
Call Signaling
Query/Response
ALI – Automatic Location Identification
ANI – Automatic Number Identification
CPE – Customer Premises Equipment
E-MF – Enhanced Multi-Frequency
ESN – Emergency Service Number
IMS – IP Multimedia Subsystem
LRF – Location Retrieval Function
MF – Multi-Frequency
MGCF – Media Gateway Control Function
MSC- Mobile Switching Center
MGW – Media Gateway
pANI – Pseudo Automatic Number Identification
PSAP – Public Safety Answering Point
SR – Selective Router
SRDB – Selective Routing Database
SS7 – Signaling System No. 7

Figure 6-6 IMS Interconnection Architecture

This architecture assumes that 9-1-1 calls are being processed by an IMS originating network. Based on the Second Report and Order, an IMS originating network is expected to support SHAKEN functionality. The application of SHAKEN to a 9-1-1 call that originates in an IMS network may result in an attestation level of "A", "B", or "C" being associated with the emergency caller's callback number. Based on current procedures related to the processing of emergency calls in an IMS network, a Proxy Call Session Control Function (P-CSCF) may, based on local policy, provide attestation information associated with the caller identity, and convey the attestation level in the SIP signaling message (e.g., in an Attestation-Info header) that it sends to downstream elements. The P-CSCF may also populate verification status information in the SIP signaling that it generates associated with an emergency call.

Since, in the context of this interconnection architecture, call delivery uses the same MF interfaces between the SR to the PSAP as in the E9-1-1 architecture, the same limitations apply with regard to the delivery of attestation level and verification status information to the legacy PSAP via the call delivery interface. Once again the ALI interface may provide a means for conveying attestation level and verification status information to legacy PSAPs that are served by this type of interconnection architecture. To support the delivery of attestation level and verification status information over the ALI interface to the legacy PSAP, the ALI system will query the LRF in the IMS network using an E2 interface upon receiving an ALI query from the legacy PSAP. If the P-CSCF has populated the attestation level and verification status information in the SIP signaling associated with the 9-1-1 call, the LRF will have this information available and could use an existing field in the E2 interface to convey it to the ALI system. The ALI system would then populate the information in an existing field in the ALI interface to convey it to the legacy PSAP. See Section 6.4 for further discussion of candidate E2 and ALI fields for use in conveying attestation level and verification status information.

It is important to note that the existing procedures related to the application of SHAKEN procedures to 9-1-1 calls that originate in IMS networks do not *require* that the P-CSCF populate attestation level and verification status information in outgoing SIP signaling. If the P-CSCF in an IMS originating network does not support this functionality, there is currently no other mechanism defined that would allow an LRF to obtain attestation level or verification status information associated with a 9-1-1 call, and as a result, no other means for conveying attestation level and verification information to a legacy PSAP that is receiving 9-1-1 calls via this interconnection architecture.

6.4 Use of ALI Data Elements for Conveyance of Attestation Level and Verification Status

As described above, limitations in the MF call delivery interfaces, and the infeasibility of updating the call processing or interfaces supported by legacy SRs suggest a need to examine the ALI interface as a means to convey attestation level and verification status information associated with callback numbers to legacy PSAPs. This Information Document presents two technically viable options for explicitly conveying attestation level and verification status information to legacy PSAPs via the ALI interface; however, it is important to note that, while ALI interface standards exist (e.g., NENA-STA-015.10-2018 [17], NENA 04-005 [18]), implementations reflect many local variations of these standards. In addition, the amount of space available and the configuration used on CPE to display call-related information to PSAP call takers varies based the type of equipment deployed.

Agencies or 9-1-1 Authorities may place different priorities on the information that is displayed to call takers, making a single solution for providing attestation level and verification status information to PSAP call takers unlikely. An objective of this Information Document is to provide Public Safety with the tools to convey caller authentication information to legacy PSAPs, should a 9-1-1 Authority or Public Safety agency determine it is desirable to do so.

As described in Section 6.1, CoS information delivered with an emergency call processed by an E9-1-1 architecture may be used to *implicitly* convey an attestation level of "A" and verification status of "TN-Validation-Passed". This is because the callback numbers associated with legacy wireline or wireless emergency originations are provided or screened by the OSP, and network-provided or "user provided, screening passed" caller identity is viewed as being the most trustworthy. So, by being able to determine, via the value in the CoS field, that the emergency call originated in a legacy wireline or wireless network, a legacy PSAP can treat the callback information as if it had an attestation level of "A" and a verification status of "TN-Validation-Passed" associated with it. Adding new values to the CoS field to support explicit conveyance of attestation level and verification status is discouraged because of the limited size of the field and the existing complexities associated with interpreting this field by legacy PSAPs.

In the case of i2/pre-i2 architectures, callback information delivered via the E2-like interface from the VPC to the legacy ALI system, and then via the ALI interface to the legacy PSAP, is also network-provided. For i2/pre-i2 VoIP networks that have implemented SHAKEN, an explicit attestation level and verification status can be conveyed via the Customer Name field that is returned by the VPC to the legacy ALI system via the v-E2 interface, and returned by the ALI system to the legacy PSAP via the legacy ALI interface. For i2/pre-i2 VoIP networks that have not implemented SHAKEN or that are not able to update the content of the Customer Name field in real-time, the legacy PSAP could determine that the attestation level and verification status are unavailable/unknown based on an explicit indication in the Customer Name field returned by the VPC. The legacy PSAP can also determine that the callback number is network-provided based on the fact that callback information was successfully retrieved from the VPC, and apply appropriate call handling based on that knowledge in accordance with SOPs.

The Customer Name field also provides a technically feasible way of conveying attestation level and verification status information to legacy PSAPs that are operating in transitional architectures that involve LPGs and LSRGs, and in architectures that support interconnection with IMS originating networks.

There is already a precedent for including more than just subscriber name information in the Customer Name field that is supported by legacy ALI and E2 interfaces.

NENA-STA-015.10-2018 (formerly NENA 02-010) [17] suggests a renaming of the "Customer Name" field to "Customer Name/Service" field to more consistently reflect how the field is currently being used and how it may be used in the future. The new "Customer Name/Service" field values defined in NENA-STA-015.10-2018 [17] are mainly used to provide guidance to the PSAP call taker regarding what location information to give priority to in handling the emergency call. The Customer Name field is currently defined to be a 32-byte alphanumeric field. Given its size and the precedent set for extending its use beyond just carrying customer name information, the Customer Name field provides a viable alternative for conveying attestation level and verification status information.

An alternative to using the Customer Name field is the Comments field. The Comments field is a 30-byte alphanumeric field that is used to convey optional notes that may be displayed to the PSAP. In practice today, the Comments field may be used to convey additional information associated with Multi-Line Telephone Systems (MLTS) users. Like the Customer Name field, the Comments field is supported by both E2 and legacy ALI interfaces, which means it could potentially be used to support the conveyance of attestation level and verification status information in the context of transitional NG9-1-1 architectures that include LPGs and egress LSRGs, as well as IMS interconnection architectures. Two advantages associated with using the Comments field to convey attestation level and verification status information are its size and the flexibility regarding the type of information that it can be used to convey. The main disadvantage associated with using the Comments field to convey attestation level and verification status information is that it is not universally deployed or consistently used. In addition, while the E2 and ALI interfaces may support the Comments field, consideration must also be given to whether there is sufficient space to display attestation and verification status information in this field to PSAP call takers.

Section 7.1 of ATIS-0500046, *Analysis of Non-IP Call Authentication Mechanisms in Support of Emergency Services* [24], proposes data formats that can be used to convey attestation level and verification status information to legacy PSAPs via the ALI/E2 interface in the Customer Name or Comments field.

7 Location Spoofing Mitigation

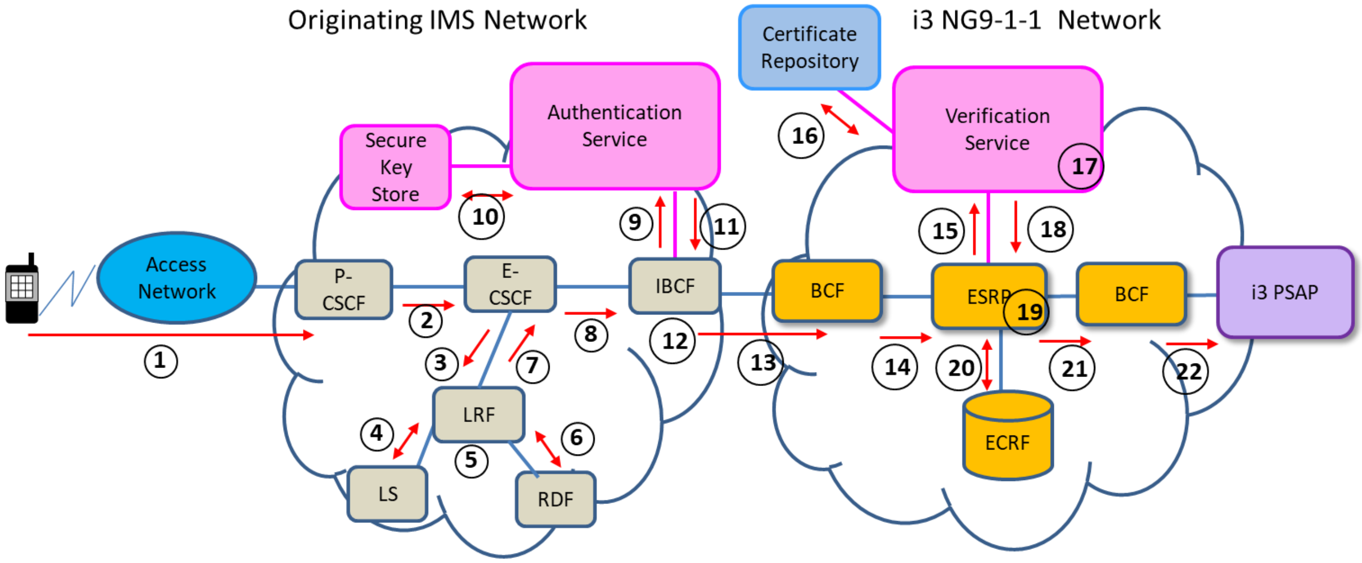
Public Safety would benefit from industry support for a mechanism, comparable to the signing/verification mechanism that has been specified for caller identity information and RPH information, that would assist the PSAP in determining whether the location information associated with a 9-1-1 call has been compromised. In an NG9-1-1 environment, emergency location is used for routing purposes as well as to support the dispatch of emergency personnel. Spoofing of emergency location can lead to the misrouting of emergency calls by the Emergency Services Network and can negatively impact emergency response. A location spoofing mitigation solution that includes the signing and verification of location information must be applicable to emergency location that is determined by the device or by the network, is conveyed "by-value" or "by-reference," and that is in geodetic or civic format. An OSP could also assert the identity of the entity responsible for providing the location URI associated with a location-by-reference. Such a solution could leverage the SHAKEN infrastructure to support the signing of location information associated with a 9-1-1 call by the OSP, and the verification of that information by the NG9-1-1 System Service Provider. By signing the location and other related information associated with a 9-1-1 call, an OSP conveys to the NG9-1-1 Emergency Services Network provider that it is responsible for asserting what it has determined regarding the location provided with the 9-1-1 call, as opposed to having the information provided by a threat agent. The conveyance of cryptographically signed assertions related to emergency location information, and associated verification status information, could support the invocation of pre-planned mitigation and recovery actions at the PSAP associated with swatting or other attacks by assisting the PSAP in identifying whether location information associated with the 9-1-1 call has been modified.

While outside the realm of spoofing mitigation, OSPs are strongly encouraged, when technically feasible, to perform a consistency check on any location that is available with an emergency call. The specific criteria used in performing the consistency check will be determined by operator policy. One example of consistency checking would be determining whether location provided by a device in the signaling associated with a cellular 9-1-1 call is in proximity to a network-determined (e.g., Phase I or Phase II) location. Consistency checking can provide input to the OSP to assist in assessing whether location information associated with a 9-1-1 call is reasonable. Including an indication of whether a consistency check was performed on location that is conveyed with a 9-1-1 call could provide downstream entities with additional information about the reasonableness of the location information that may be useful in processing those calls.

7.1 High Level Call Flows

7.1.1 9-1-1 Origination with Signed Caller Identity, RPH, and Location

Figure 7-1 illustrates a call flow based on the architecture shown in Figure 5-1. Figure 7-1 depicts a scenario where an emergency call is originated by a mobile device (e.g., a smartphone) and is processed by an IMS originating network. The mobile device provides location-by-value in the signaling associated with the emergency call. SHAKEN caller identity authentication, RPH signing, and location checking and signing is performed on the information signaled with the emergency call. Location-based routing performed by the originating network determines that the emergency call is to be routed via an i3 ESInet/NGCS.



BCF – Border Control Function
ECRF – Emergency Call Routing Function
E-CSCF – Emergency Call Session Control Function
ESRP – Emergency Service Routing Proxy
IBCF – Interconnection Border Control Function

LRF – Location Retrieval Function
LS – Location Server
P-CSCF – Proxy Call Session Control Function
RDF – Routing Determination Function

Figure 7-1 9-1-1 Origination: Caller Identity, RPH and Location Signing/Verification

Step 1. The originating mobile device, which is authenticated to the P-CSCF, creates a SIP INVITE message that includes a callback number (i.e., a telephone number identity), an sos service URN, and location information in the form of a Presence Information Data Format – Location Object (PIDF-LO) in the body of the message (i.e., location-by-value).

Step 2. The P-CSCF in the originating network adds an RPH set to "esnet.1" to the SIP INVITE message, along with Attestation-Info and Origination-Id header fields for use by downstream calling identity authentication and verification processes. The P-CSCF may also include a "verstat" parameter in the SIP INVITE message, if supported by local policy. The P-CSCF passes the SIP INVITE to the E-CSCF.

Step 3. The E-CSCF passes the SIP INVITE message to the LRF to obtain location and routing information for the emergency call.

Step 4. The LRF interacts with an LS to acquire initial (Phase I) location and to initiate position determination, and the LS responds with the initial location information.

Step 5. The LRF performs a consistency check that compares the device-provided location to the initial location provided by the LS. In this call flow example, the device-provided location is within the serving area of the Phase I location.

Step 6. The LRF queries the RDF using location information and an sos service URN. Whether the LRF uses the device-based location or an Associated Location[9] as input to the routing process is left to local policy. The RDF returns a Route URI. In this example, the Route URI is associated with an ESRP in an i3 ESInet.

Step 7. The LRF redirects the call back to the E-CSCF by returning a 300 Multiple Choices message that includes a Route URI that directs the call toward the i3 ESInet/NGCS. In this example, the 300 Multiple Choices message also contains the device-based location and, based on operator policy, a network-determined location (e.g., Phase I location) "by-value," a location URI (i.e., location-by-reference to support requests for location updates), and Additional Data.

Step 8. The E-CSCF generates an outgoing SIP INVITE message, using the information received from the LRF as well as information received in the initial SIP INVITE message, and forwards it to the exit IBCF. In this example the SIP INVITE includes the sos service URN, a Route URI, location-by-value, location-by-reference, the callback number with associated "verstat" information, an Attestation-Info header, an Origination-Id header, the RPH, and Additional Data.

Step 9. The exit IBCF interacts with the Authentication Service, requesting that it sign the caller identity information, the RPH, and the location information that it received in the SIP INVITE message.

Step 10. The Authentication Service securely requests its private key from the Secure Key Store, and the Secure Key Store provides the private key in response.

[9] An Associated Location is a location (civic, geodetic, or polygon) within the designated PSAP jurisdiction that may be used in wireless call scenarios to route the call toward the designated PSAP. An LRF determines an Associated Location by mapping a cell ID to a routing location that is associated with the PSAP that, based on pre-existing agreements, is supposed to receive the call.

Step 11. The Authentication Service uses the key to sign the caller identity, RPH, and location information then returns signing response messages with the signed information.

Step 12. The exit IBCF uses the information returned by the Authentication Service to populate SIP Identity headers associated with the caller identity (callback number), the RPH, and the location information in the SIP INVITE message. The IBCF also removes the "verstat," if present, prior to sending the call to the i3 ESInet.

Step 13. The exit IBCF then routes the SIP INVITE to the ingress BCF at the edge of the ESInet.

Step 14. The BCF performs protocol checks on the received SIP INVITE message. It also checks that the RPH is present and that is contains a value of "esnet.1". The BCF then forwards the SIP INVITE message to the ESRP.

Step 15. The ESRP in the i3 ESInet forwards the received SIP INVITE message to the Verification Service.

Step 16. The Verification Service interacts with the Certificate Repository to obtain the certificate used to sign the caller identity, RPH, and location information.

Step 17. The Verification Service validates the certificate and then extracts the public key. It uses the public key to verify the signature in the Identity header fields, which validate the caller identity, RPH, and location information content signed by the originating network Authentication Service.

Step 18. The Verification Service returns the SIP INVITE message to the ESRP. The SIP INVITE message includes a "verstat" parameter indicating the verification status of the caller identity information, and a Priority-Verstat header field indicating the result of the verification of the RPH information. The mechanism for conveying verification status information associated with signed location information is for further study.

Step 19. Since, in this example, both location-by-value and location-by-reference are provided in the SIP INVITE associated with the emergency call, the ESRP will determine which location to use for routing based on policy. If the ESRP determines that the location-by-reference is to be used, it will query the LRF (as identified in the location URI) for routing location (not shown).

Step 20. The ESRP queries the ECRF for routing information using the routing location and an sos service URN. The ECRF returns a Route URI (i.e., PSAP URI) in response.

Step 21. The ESRP passes the SIP INVITE message to the BCF on the egress side of the ESInet/NGCS. In this example the SIP INVITE includes an sos service URN, a Route URI (associated with the i3 PSAP), location-by-value, location-by reference, the callback number with associated "verstat" information, an Attestation-Info header, an Origination-Id header, the RPH, a Priority-Verstat header field, the Identity headers, Additional Data, and verification status information associated with the signed location information.

Step 22. The BCF passes the SIP INVITE message to the i3 PSAP.

7.2 Open Issues

The protocol to support the signing and verification of location information requires further study. Leveraging the SHAKEN reference architecture, SIP signaling elements that carry location information (e.g., PIDF-LO, Geolocation header) could be included in a signing request sent to an Authentication Service by an element in the originating network (e.g., the IBCF), using a mechanism that is similar to the one used to sign the Resource-Priority Header information associated with an emergency call. Signing a PIDF-LO would result in the PIDF-LO appearing in both the body of the SIP INVITE message associated with an emergency call as well as in an Identity header in the same message. Due to concerns regarding message size, an alternative approach would be to create a hash of the PIDF-LO and sign the hash rather than the PIDF-LO itself. Creating and signing a hash of the PIDF-LO are for further study. Any changes involving the PIDF-LO will require the involvement of the IETF.

IETF activity will also be required to define an applicable PASSporT extension to support signing and verification of location and related information. In addition, extensions to SIP will be needed to convey the verification results associated with signed location information forward to the PSAP. Activity in 3GPP will likely be required to define the SIP extensions needed to convey verification results, as well as to define extensions to the HTTP messaging used to support the signing and verification of location information.

8 Operational Impacts/Considerations Associated with Applying Spoofing Mitigation Techniques to 9-1-1 Calls and Emergency Callbacks

8.1 Definition of new SOPs

Spoofing mitigation, as well as consistency checking of location information, shall be addressed in SOPs either to influence call handling or to support post-processing associated with the call, depending on the jurisdiction. These SOPs should be put in place and appropriate training provided before the spoofing mitigation technologies are implemented and new information, such as attestation levels, is delivered with emergency calls. Policies related to support for spoofing mitigation technologies will be subject to review prior to adoption by a given agency, and will be subject to periodic reviews and updates. The spoofing mitigation portion of the agency's SOP will clearly define how the agency will handle attestation levels and verification status information, and the circumstances under which they apply. The SOP will also need to define how the agency will use consistency check indicators associated with location information in processing incoming 9-1-1 calls. Actions and responsibilities for Telecommunicators and other staff need to be clearly defined. All agency-identified common issues and actions need to be addressed. Listed below are some examples of each. These should be evaluated against the use cases provided along with any additional agency-defined use cases.

Some examples of common issues that are addressed in SOPs today include the following:

- Signal/connection loss.
- Caller abruptly disconnected before caller and/or location information can be verified.
- Caller is unable to provide and/or verify information.
- Unintentional dialing of 9-1-1 sometimes referred to as pocket dialing.
- Non-verbal caller. This may be related to the nature of the emergency, a physical limitation, or a technical problem.
- Callers reporting a threat such as a bomb threat or an active shooter.

The Use Cases described in Section 5.1, the caller authentication mechanisms described in Section 6, and the location spoofing mechanism described in Section 7, can provide input to the development of SOPs, taking into account potential impacts on the following actions due to the availability of additional information such as the attestation level associated with the callback number and verification status associated with the callback number and location information. Not all of the actions listed below will apply to all of the issues identified above, but these actions could be considered in developing SOPs that address spoofing mitigation. Some examples of actions that need to be addressed (some may be by the call taker, and some by others) include the following:

- Record the information received such as date and time of the call, call taker and station taking the call, all information presented to the call taker, all information missing, and any abnormalities or other observations.
- What, if any, differences there are based on what is currently happening and the attestation level of the call(s). This defines how the agency will prioritize and handle calls of different attestation levels in relation to other calls occurring around the same time.

- Escalation process with contacts.
- Contacting a Network Operation Center (NOC). This may be your agency's, vendor's, carrier's, or a combination of them.
- Evaluation of call records. This may be through information presented to the call taker or through information obtained through other technical sources.
- Process and procedures for preserving forensic information for potential future litigation. This must follow "chain of custody" procedures to remain valid for litigation.

8.2 PSAP Training

All staff shall be trained on their roles and responsibilities as defined in the SOP. This training shall include what is expected of them in relation to spoofing mitigation, how the agency will handle differing attestation levels, and how the agency will utilize consistency check indicator values associated with location information received with 9-1-1 calls. Periodic refresher training will be conducted. General training regarding SHAKEN caller authentication including attestation levels and verification status values, as well as digital certificates and the PSAP Credentialing Agency (PCA) would be beneficial as part of the training provided to agency staff.

8.3 Integration with existing cybersecurity infrastructure

A risk assessment and evaluation will be conducted in accordance with the agency's policies and procedures prior to introducing any new technology or practices for spoofing and mitigation. This includes the agency's procedures for handling calls in relation to the attestation level associated with the callback number, and the verification status associated with the callback number and location, which will be subject to local policies and/or regulation. See NENA-STA-040.2-202Y [15] for further details regarding security considerations in an NG9-1-1 environment.

8.4 Impacts on Display of Call/Caller Information

The application of SHAKEN caller identity authentication and verification and non-IP caller authentication mechanisms to 9-1-1 calls will result in additional information being displayed to the PSAP call taker on their CPE. It is expected that when SHAKEN or non-IP caller authentication 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. Likewise, the application of signing/verification to location information and the conveyance of consistency check indicators will result in additional information being displayed to the PSAP call taker. The ability to display attestation level information, verification status information, and consistency check indicators to call takers will be constrained by PSAP equipment limitations. Call/Caller information display impacts will likely be a consideration in an NG9-1-1 environment in general, as more data becomes available with emergency calls. Enhancements to existing PSAP equipment may be needed to accommodate the display of additional call-related information. Vendors should design their equipment in coordination with the PSAPs to allow data display to be easily extensible, as NG9-1-1 evolves and additional call-related information becomes available. In addition, equipment design should accommodate variations in the way that displays are formatted to meet the needs of individual Public Safety agencies.

New Methods and Procedures will need to be defined to specify how attestation level, verification status information, and consistency check indicators 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 their displays. For i3 PSAPs, this will include scenarios where expected information is not available for display. When such a scenario exists, an explicit indication should be provided to the call taker to indicate the unavailability of information. This will allow the call taker to distinguish between scenarios where the information was not delivered to the Call Handling Equipment in the signaling associated with the emergency call, and PSAP equipment errors.

For legacy PSAPs, the SOPs will need to specify which existing ALI field the PSAP call taker should look at to identify the attestation level and verification status associated with the callback number provided with the 9-1-1 call. If such information is not available with a 9-1-1 call, either an explicit indication that the information is unavailable should be provided via the ALI interface or the information will be omitted from the ALI data delivered to the legacy PSAP for the call.

8.5 Outgoing Calls from PSAPs

There are different types of outgoing calls that may be originated by a PSAP. This section addresses operational considerations with regard to emergency callbacks, Emergency Support Calls (e.g., from one Public Safety Agency to another, associated with an incident), and "other" (i.e., non-emergency) outgoing calls. It is important to note that the considerations described in this section also apply to PSAPs at backup sites.

8.5.1 Emergency Callbacks

Section 5 describes the signaling and alternative architectures involved in processing emergency callbacks that are originated by i3 PSAPs and routed via an ESInet. As described in Section 5, emergency callbacks are expected to include additional information in the SIP signaling generated by the Call Handling function (i.e., the RPH and Priority header) in addition to the caller identity information (which in the case of an emergency callback identifies the PSAP originating the call). To mitigate spoofing of this information, authentication and verification procedures are expected to be applied as described in Section 3 and Section 5 of this document.

From an operational standpoint, it is important that the user interface and the Call Handling Functional Element (FE) associated with an i3 PSAP support, and that SOPs define, the mechanism by which a PSAP call taker can request the establishment of a callback call. The mechanism used by a PSAP to request an emergency callback (whether via explicit action by the PSAP or by having equipment automatically initiate a callback based on the detection of a disconnect from the emergency caller with a subsequent display to the call taker[10]) must be specified and result in the Call Handling FE generating an emergency callback, via the desired network, with the appropriate information included in outgoing signaling so that authentication and verification of that information can be performed downstream. The SOPs must also provide guidance as to whether, or under what conditions, the PSAP caller identity should be kept private, and the user interface must support a mechanism for conveying a request for privacy of caller identification to the Call Handling FE.

While it is expected that agencies that support i3 PSAP functionality will typically route emergency callbacks via an ESInet (and will be required to do so in the case of multimedia callbacks), it is possible that an agency may route an emergency callback via a VoIP carrier network or the PSTN, based on local policy. Agencies that allow emergency callbacks to be routed via a network other than an ESInet must also identify in their SOPs 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 by the Call Handling FE. When an emergency callback is routed via a VoIP carrier network, it is expected that SHAKEN call authentication and RPH and Priority header signing procedures will apply. If an emergency callback is to be routed via a VoIP carrier network, then in order to achieve "A" level attestation, the caller identity (i.e., the PSAP calling number) must be populated with a telephone number that was assigned to the PSAP by the VoIP carrier over whose network the call is to be routed. If the caller identity (i.e., the PSAP calling number) consists of a telephone number that was assigned to the PSAP by a different carrier than the one over whose network the emergency callback is being routed, it is expected that either a "B" or "C" level attestation will be associated with the caller identity. It is expected that emergency callbacks initiated by legacy PSAPs will continue to be routed via the PSTN.

If an emergency callback is routed via the PSTN, non-IP caller authentication mechanisms may be applied to the call, in accordance with the FCC Second Report and Order, in the originating, transit or terminating network. (As described in Section 3.1.1.5, the FCC

[10] NENA standards related to NG9-1-1 PSAPs do not currently support an "automatic callback" mechanism.

Second Report and Order [9] requires that non-IP voice service providers must, by June 30, 2021, be able to prove that they are actively working to develop a non-Internet Protocol caller identification authentication solution.) Since legacy signaling protocols do not support the conveyance of a specific indicator identifying a call as callback call, the conveyance of a SIP Priority header with a value of "psap-callback", and the signing of this information will not be possible if an emergency callback is initially routed via the PSTN. There is also no standard mapping from legacy signaling protocols used in the context of emergency callbacks to the SIP RPH, so authentication/verification of the RPH in SIP-based transit or terminating networks will also not apply to callback calls generated by legacy PSAPs.

Note that routing of emergency callbacks via networks other than ESInets must meet recording and priority handling (where applicable) requirements associated with emergency callbacks.

8.5.2 Emergency Support Calls

Emergency Support Calls are typically viewed as being between Public Safety agencies or between Public Safety Agencies or another entity that is relevant to the processing of an incident, and are characterized by the need for recording of media associated with the call. Emergency Support Calls originated by i3 PSAPs may or may not be routed via an ESInet, and if routed via an ESInet, may be intra-ESInet or inter-ESInet. It is important to note that the routing of an Emergency Support Call will be influenced by the need to record the call. For intra-ESInet calls, caller identity should be authenticated and a verification status ('verstat') populated, following the mechanisms defined for intranetwork SHAKEN. While Emergency Support Calls are expected to include an RPH, intra-ESInet official calls will not be subject to RPH signing.

For Emergency Support Calls sent to an agency served by a different ESInet (i.e., inter-ESInet calls) it is expected that the call information (caller identity and RPH [if present in signaling from Call Handling FE]) will be authenticated in the same way as for an emergency callback, except that there will be no Priority header populated for an Emergency Support Call.

For Emergency Support Calls that are routed via a VoIP carrier network (i.e., not an ESInet), it is expected that normal caller identity SHAKEN authentication and verification procedures would apply. While an RPH is not expected to be signaled for Emergency Support Calls routed via a network other than an ESInet, if an RPH is populated in outgoing signaling by the Call Handling FE for such calls, RPH signing/verification may also apply. As for emergency callbacks, it is unlikely that an "A" level attestation will be associated with the caller identity information signaled with an Emergency Support Call unless the telephone number populated as the caller identity was assigned by the carrier over whose network the call is being routed.

Emergency Support Calls routed via the PSTN will not be subject to SHAKEN authentication/verification or RPH or Priority header signing/verification. Emergency Support Calls initiated by legacy PSAPs are expected to be routed via the PSTN. Emergency Support Calls routed via the PSTN are expected to be subject to whatever non-IP caller authentication mechanisms may be implemented in the originating, transit and terminating networks traversed by the call.

As with emergency callbacks, SOPs will need to provide guidance to PSAP call takers regarding the mechanism by which they can request the establishment of an Emergency Support Call. This capability must be supported by the user interface. For i3 PSAPs, sufficient information must be conveyed to the Call Handling FE to allow it to select an appropriate outgoing route (i.e., one that supports recording) and to populate information in the outgoing signaling correctly. If an agency wishes to allow caller identity to be kept private on official calls, the SOPs must also provide guidance as to the conditions under which the PSAP caller identity should be kept private. For i3 PSAPs, the user interface must support a mechanism for conveying a request for privacy of caller identification to the Call Handling FE.

8.5.3 Outbound Non-Emergency Calls

It was noted that the handling/routing of non-emergency calls by PSAPs will depend on equipment implementation and SOPs. It is unlikely that Call Handling equipment will be able to distinguish between outgoing calls to non-official destinations and Emergency Support Calls or emergency callbacks based on the target destination. As a result, non-emergency calls initiated by i3 PSAPs may be routed via the ESInet, just like Emergency Support Calls and emergency callbacks. It is expected that Emergency Support Calls and emergency callbacks that are routed via the ESInet will have an RPH associated with them, but non-emergency calls will not.

If, based on input provided via the user interface (e.g., something that mirrors the functionality associated with key systems in use today), and in accordance with SOPs, it is determined that a certain type of outgoing call is to be routed via the legacy PSTN, it is expected that such calls will be subject to the non-IP caller authentication mechanisms implemented by the originating, transit or terminating networks traversed by the call. Outbound calls initiated by legacy PSAPs are expected to be routed via the PSTN.

If the outgoing call is to be routed via a VoIP carrier network (and not the ESInet), it is expected that normal SHAKEN caller identity authentication and verification procedures will be applied to the call. Non-emergency calls routed via a VoIP carrier network are not expected to have an RPH or SIP Priority header associated with them, so signing and verification of that information will not be performed. As with emergency callbacks and Emergency Support Calls, it is unlikely that the caller identity associated with other PSAP-originated calls routed via a VoIP carrier network will achieve an attestation level of “A” unless the caller identity consists of a telephone number that was assigned by the carrier over whose network the call is routed.

Also, as with emergency callbacks and Emergency Support Calls, SOPs will describe whether there are circumstances under which the caller identity associated with other (non-emergency) outgoing calls should be kept private. If this capability is supported by the SOPs, the user interface must support a mechanism for conveying a request for privacy of caller identification to the serving switch or Call Handling FE for other (non-emergency) calls.

9 Conclusion/Recommendations

Concerns regarding the illegitimate spoofing of information that is critical to the handling of emergency calls and callback calls may be addressed by applying the SHAKEN caller identity spoofing mitigation framework and RPH, and location signing/verification procedures to 9-1-1 calls, and caller identity spoofing mitigation and RPH and Priority header signing/verification to emergency callbacks in an end-state NG9-1-1 environment. Likewise, illegitimate spoofing of caller identity and RPH information may be addressed by non-IP call authentication mechanisms in the context of E9-1-1, transitional NG9-1-1, and IMS interconnection architectures. However, additional work is needed to address gaps in functionality and to address the operational impacts associated with the application of information spoofing mitigation techniques.

9.1 Areas of Future Work

Sections 5.3 and 7.2 describe open issues related to the application of spoofing mitigation mechanisms to 9-1-1 calls and emergency callbacks, and the application of consistency checking to emergency location associated with 9-1-1 calls. Resolution of these open issues will require future work in the following areas.

Since there is a need, under certain circumstances, to be able to keep PSAP calling numbers private (i.e., not displayed to the called party) when placing emergency callbacks, future work will need to focus on specifying a standard mechanism by which the ‘verstat’ can be delivered to the called UE, even though the calling number is kept private. Delivering the verification status associated with the calling number may improve the probability that the emergency callback will be answered by the emergency caller. The standard SIP signaling mechanism for delivering the verification status of a calling number uses a parameter associated with a tel URI. However, when a calling number is kept private, the calling information delivered to the called party consists of a sip URI formatted as sip:anonymous@anonymous.invalid. There is currently no standard way of including a parameter (e.g., to convey verification status) with a sip URI. Resolution of this issue will require activity within IETF to explicitly allow parameters to be included with sip URIs. While this problem is not unique to emergency callbacks (i.e., this issue applies to any call where the calling number is to be kept private) resolution of this issue is needed to allow verification status information ('verstat') associated with a private caller identity to be delivered to the emergency caller associated with an emergency callback.

Public Safety must deal with situations where caller location information is spoofed, resulting in significant risks to life and property. As described in Section 7, a location spoofing mitigation solution could leverage the SHAKEN infrastructure to support the signing of location information associated with a 9-1-1 call by the OSP, and the verification of that information by the NG9-1-1 System Service Provider. The protocol to support the signing and verification of location information requires further study. IETF activity will be required to define an applicable PASSporT extension to support signing and verification of location and related information. Activity in 3GPP will also be needed to define extensions to the HTTP messaging used to support the signing and verification of location information.

In addition, future work is needed to define a way to communicate verification results associated with signed location information in SIP signaling. As discussed in Section 7.2, this will require the appropriate SIP protocol extensions to support the conveyance of verification results related to location information under various call scenarios.

9.2 Summary of SOP Impacts

Spoofing Mitigation will be addressed in SOPs either to influence call handling or to support post-processing associated with an emergency call, depending on the jurisdiction. The spoofing mitigation portion of an agency's SOP should clearly define how attestation level and verification status information should be used by a PSAP in the course of handling an emergency call and where the new information will appear on their displays. Likewise, the availability of consistency check-related information may influence call handling and the dispatch of emergency personnel, as well as supporting post-processing associated with 9-1-1 calls. SOPs will need to address the use of this information and where it will appear on PSAP displays. These SOPs should include: an identification of the received call-related information that should be recorded (e.g., date and time of the call, call taker and station taking the call, all information presented to the call taker, all information missing, and any abnormalities or other observations); a description of how an agency will prioritize and handle calls of different attestation levels and with different verification status values in relation to other calls occurring around the same time; a description of how consistency check-related information will be used; a specification of the escalation process, including appropriate contact information; identification of the circumstances under which a NOC is to be contacted and specification of whose NOC it is (i.e., the agency's, their vendor's, their carrier's, or a combination of them). In addition, SOPs should describe a mechanism for evaluating call records that include information presented to the call taker and/or information obtained through other technical sources. SOPs should also specify the processes and procedures for preserving forensic information for potential future litigation, following "chain of custody" procedures to remain valid for litigation.

With regard to outgoing calls, SOPs should define the mechanism by which a PSAP call taker can request the establishment of an outgoing call (i.e., callback call, Emergency Support Call, or non-emergency 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., 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). In addition, based on local policy, SOPs may specify what calling number(s) should be used by the PSAP for a particular type of outgoing call and provide guidance as to whether, or under what conditions, the PSAP caller identity should be kept private when generating an outgoing call.

10 Impacts, Considerations, Abbreviations, Terms, and Definitions

10.1 Operations Impacts Summary

As discussed in Section 8, spoofing mitigation will need to be addressed in SOPs either to influence call handling, dispatch, or to support post-processing associated with emergency calls, depending on the jurisdiction. Staff should be trained to understand what is expected of them in relation to spoofing mitigation and how the agency will handle differing attestation levels and verification status values. The application of spoofing mitigation to 9-1-1 calls will result in impacts to displays on PSAP equipment. Likewise the ability to receive consistency check-related information will impact PSAP equipment displays. Call takers will need to be trained to work with the new information and to recognize where it will appear on the new displays. In addition, SOPs should define the mechanism by which a PSAP call taker can request the establishment of an outgoing call whether it be an emergency callback, an Emergency Support Call, or a non-emergency call. This should include the means by which the PSAP designates the calling number to be used for the call, and the ability to request that the calling number be kept private.

10.2 Technical Impacts Summary

While NENA-STA-010.3 [12] addresses the validation of caller identity information in incoming 9-1-1 calls and the authentication of caller identity information associated with emergency callbacks, the i3 ESInets/NGCS will be further impacted by the need to support the signing/verification of RPH and Priority header information. In addition, a Call Handling FE in an i3 PSAP must be capable of receiving and processing a SIP INVITE that contains attestation level and verification status information. As discussed in Section 8.4, there will also be impacts to PSAP equipment to support display of information related to spoofing mitigation associated with 9-1-1 calls. The Call Handling FE must also be capable of interpreting requests for outgoing calls from i3 PSAPs and routing and populating the outgoing signaling information associated with those calls appropriately.

Processing at LPGs and egress LSRGs will be impacted by the use of ALI data fields to convey attestation level and verification status information associated with an emergency caller's identity to legacy PSAPs in a transitional NG9-1-1 environment.

10.3 Security Impacts Summary

Attestation level and verification status information has the potential to be a useful tool that can be used in helping in mitigating malicious activities with inbound 9-1-1 calls. It is important to note that SHAKEN-based spoofing mitigation solutions are not fool-proof, and there may exist methods that can be used to mask or defeat the caller identity attestation process. For an example of this, think of how the current process works when a call goes through a service that hides the original caller. There are others and you can be assured that bad actors are looking into them. This does not mean that attestation level is not useful but take care that its weaknesses are understood as well.

When developing policies and procedures that perform mitigation activities, make sure that they comply with all applicable governance. Perform risk assessments for how mitigation activities are going to treat calls when using the attestation level and verification status information and how any mitigation steps will interact with an existing 9-1-1 network. Make sure your supervisor(s) and/or governing board understand and accept these risks.

10.4 Recommendation for Additional Development Work

While NENA-STA-010.3 [12] addresses the authentication and verification of caller identity information, a future issue of NENA-STA-010 will address the signing/verification of RPH and Priority header information, and spoofing mitigation in the context of emergency call transfers. NG9-1-1 PSAP Standards will also need to address support for spoofing mitigation procedures and data.

As described in Section 9.1, future work will be needed in IETF and 3GPP to specify the protocol enhancements needed to support the location spoofing mitigation mechanism described in this document.

In addition, based on the provisions of the Second Report and Order, future work should consider potential impacts on Legacy Network Gateways and ingress LSRGs to support call authentication in transitional NG9-1-1 environments, where part of the service architecture is not IP/SIP-capable. This could impact NENA standards related to gateway functional elements.

10.5 Anticipated Timeline

The FCC Second Report and Order [9], released on October 1, 2020, requires that voice service providers support the STIR/SHAKEN caller ID authentication framework in the IP portions of their networks by June 30, 2021. The Second Report and Order [9] also requires that, by June 30, 2021, non-IP voice service providers either upgrade their networks to support SIP calls and fully implement SHAKEN throughout its network, or that they, upon request of the FCC, provide documented proof that they are participating as members of a working group, industry standards group, or consortium that is working to develop a non-IP caller identification authentication solution. Consistent with the Gateway Provider Report and Order [23] described in Section 3.1.1.6, the FCC requires that, by June 20, 2023, gateway providers apply STIR/SHAKEN caller ID authentication in the IP portions of their networks to all unauthenticated foreign-originated SIP calls that have U.S. North American Numbering Plan (NANP) calling numbers. It is expected that i3 ESInet/NGCS implementations will support SHAKEN caller identity spoofing mitigation standards in accordance with 2- to 5-year implementation schedule described in NENA-STA-010 [12], consistent with other i3-related upgrades. Support for implementation of SHAKEN caller identity spoofing mitigation procedures by NG9-1-1 PSAPs, and RPH signing and verification by i3 ESInets/NGCSs will depend on the availability of published standards.. Support for caller authentication in an E9-1-1 or transitional NG9-1-1 environment will depend on the availability of non-IP call authentication solutions that accommodate the unique signaling and architectural characteristics of legacy E9-1-1 and transitional NG9-1-1 service architectures, as described in ATIS-0500046 [24]. Implementation of location spoofing mitigation in an end state NG9-1-1 environment will be dependent on the development of standards that define the procedures and protocols necessary to support the signing and verification of emergency location information.

10.6 Cost Factors

At this time, it is difficult to predict the costs of system upgrades required to support the spoofing mitigation mechanisms described in this document. Vendors and service providers must determine the impact of supporting the spoofing mitigation procedures, interfaces, and data described in this document and in associated standards on their products and operations.

10.7 Cost Recovery Considerations

Cost recovery mechanisms are dependent on local PSAP or 9-1-1 Authority governance models.

10.8 Additional Impacts (non-cost related)

The information contained in this NENA document is expected to have both 9-1-1 technical and operational impacts, based on the analysis of the authoring group. The implementation of the spoofing mitigation mechanisms described in this document will impact the 9-1-1 system and associated Public Safety policies related to changes in network and PSAP systems, interfaces, procedures, and data. Additional analysis may be necessary to determine if there are any non-cost related impacts that were not considered during the development of this document as associated standards are developed and implementations become available.

11 Abbreviations, Terms, and Definitions

See the NENA Knowledge Base (NENAkb) [1] for a Glossary of terms and abbreviations used in NENA documents. Abbreviations and terms used in this document are listed below with their definitions.

Term or Abbreviation (Expansion)	Definition / Description
3GPP (3rd Generation Partnership Project)	A collaboration agreement that was established in December 1998. The collaboration agreement brings together a number of telecommunications standards bodies which are known as "Organizational Partners."
ALI (Automatic Location Identification)	The automatic display at the PSAP of the caller's telephone number, the address/location of the telephone, and supplementary emergency services information of the location from which a call originates.
ANI (Automatic Number Identification)	Telephone number associated with the call origination, originally associated with the access line of the caller.
ATIS (Alliance for Telecommunications Industry Solutions)	A U.S.-based organization that is committed to rapidly developing and promoting technical and operational standards for the communications and related information technologies industry worldwide using a pragmatic, flexible, and open approach.

Term or Abbreviation (Expansion)	Definition / Description
BCF (Border Control Function)	Provides a secure entry into the ESInet for emergency calls presented to the network. The BCF incorporates firewall, admission control, and may include anchoring of session and media as well as other security mechanisms to prevent deliberate or malicious attacks on PSAPs or other entities connected to the ESInet.
CAMA (Centralized Automated Message Accounting)	A type of in-band analog transmission protocol that transmits telephone number via multi-frequency encoding. Originally designed for billing purposes.
CISC (CRTC Interconnection Steering Committee)	The Steering Committee for the CRTC (Canadian Radio-Television and Telecommunications Commission).
CoS (Class of Service)	A designation in E9-1-1 that defines the service category of the telephony service. A few examples are residential, business, Centrex, coin, PBX, VoIP and wireless Phase II (WPH2).
CPE (Customer Premises Equipment)	Communications or terminal equipment located in the customer's facilities – Terminal equipment at a PSAP.
CRTC (Canadian Radio-television and Telecommunications Commission)	Supervises and regulates broadcasting and telecommunications systems in Canada.
CSCF (Call Session Control Function)	General term for a functional entity within a IMS core network that can act as Proxy CSCF (P-CSCF), Serving CSCF (S-CSCF), or Emergency CSCF (E-CSCF).
ECRF (Emergency Call Routing Function)	A functional element in NGCS (Next Generation Core Services) which is a LoST (Location-to-Service Translation) protocol server where location information (either civic address or geo-coordinates) and a Service URN serve as input to a mapping function that returns a URI used to route an emergency call toward the appropriate PSAP for the caller's location or towards a responder agency.
E-CSCF (Emergency Call Session Control Function)	The entity in the IMS core network that handles certain aspects of emergency sessions, e.g., routing of

Term or Abbreviation (Expansion)	Definition / Description
	emergency requests to the correct emergency center or PSAP.
Enhanced MF (Enhanced Multi-Frequency)	A signaling protocol, used on the E9-1-1 tandem-to-PSAP interface, that is based on the Feature Group D (FG-D) protocol and supports the delivery of up to two 10-digit numbers, the first of which is preceded by two ANI information digits (i.e., ANI "II" digits).
ESGW (Emergency Services Gateway)	The Emergency Services Gateway (ESGW) is the signaling and media interworking point between the IP domain and conventional trunks to the E9-1-1 SR that use either Multi-Frequency (MF) or Signaling System No. 7 (SS7) signaling. The ESGW uses the routing information provided in the received call setup signaling to select the appropriate trunk (group) and proceeds to signal call setup toward the SR using the ESQK (Emergency Services Query Key) to represent the Calling Party Number/Automatic Number Identification (ANI) information.
ESInet (Emergency Services IP Network)	An ESInet is a managed IP network that is used for emergency services communications, and which can be shared by all public safety agencies. It provides the IP transport infrastructure upon which independent application platforms and core services can be deployed, including, but not restricted to, those necessary for providing NG9-1-1 services. ESInets may be constructed from a mix of dedicated and shared facilities. ESInets may be interconnected at local, regional, state, federal, national, and international levels to form an IP-based internetwork (network of networks). The term ESInet designates the network, not the services that ride on the network. See NG9-1-1 Core Services.
ESN (Electronic Serial Number)	A unique code created to identify mobile devices.
ESRK (Emergency Services Routing Key)	A 10-digit North American Numbering Plan number that uniquely identifies a wireless emergency call, is used to

Term or Abbreviation (Expansion)	Definition / Description
	route the call through the network, and used to retrieve the associated ALI data.
ESRP (Emergency Service Routing Proxy)	An i3 functional element which is a SIP proxy server that selects the next-hop routing within the ESInet based on location and policy. There is an ESRP on the edge of the ESInet. There is usually an ESRP at the entrance to an NG9-1-1 PSAP. There may be one or more intermediate ESRPs between them.
ESWG (Emergency Services Working Group)	A Working Group under CISC composed of Telecommunication Service Providers, Public Safety Answering Points (PSAPs), and 9-1-1 Industry specialists responsible for addressing issues that relate to the provisioning of 9-1-1 services, including the technical and operational implementation of 9-1-1 services.
ESZ (Emergency Service Zone)	A geographical area that represents a unique combination of emergency service agencies (e.g., Law Enforcement, Fire, and Emergency Medical Service) that is within a specified 9-1-1 governing authority's jurisdiction. An ESZ can be represented by an Emergency Service Number (ESN) to identify the ESZ.
FCC (Federal Communications Commission)	An independent U.S. government agency overseen by Congress, the commission is the United States' primary authority for communications law, regulation, and technological innovation. The FCC regulates interstate and international communications by radio, television, wire, satellite, and cable in all 50 states, the District of Columbia, and U.S. territories.
FE (Functional Element)	An abstract building block that consists of a set of interfaces and operations on those interfaces to accomplish a task. Mapping between functional elements and physical implementations may be one-to-one, one-to-many, or many-to-one.
FNPRM (Further Notice of Proposed Rulemaking)	The mechanism by which the FCC provides an opportunity for consumers to provide comments regarding proposed changes to the Commission's rules

Term or Abbreviation (Expansion)	Definition / Description
	or specific issues raised in comments related to previously proposed changes.
HTTP (Hypertext Transfer Protocol)	Hypertext Transfer Protocol is typically used between a web client and a web server that transports HTML and/or XML.
i3 PSAP (i3 Public Safety Answering Point)	A PSAP that is capable of receiving IP-based signaling for delivery of emergency calls and for originating calls and is conformant to NENA specifications for such PSAPs.
IBCF (Interconnection Border Control Function)	An IBCF provides application-specific functions at the SIP/Session Description Protocol layer in order to perform interconnection between two operator domains. It enables communication between Ipv6 and Ipv4 SIP applications, network topology hiding, controlling transport plane functions, screening of SIP signaling information, selecting the appropriate signaling interconnect, and generation of charging data records. See 3GPP TS 23.002. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=728
IETF (Internet Engineering Task Force)	Lead standard-setting authority for Internet protocols.
IMEI (International Mobile Equipment Identity)	A 15- or 17-digit code that uniquely identifies mobile phone sets. The IMEI code can enable a GSM (Global System for Mobile communication) or UMTS (Universal Mobile Telecommunications Service) network to prevent a misplaced or stolen phone from initiating calls.
IMS (IP Multimedia Subsystem)	A reference architecture defined by 3GPP that comprises all 3GPP/3GPP2 core network elements providing IP multimedia services that support audio, video, text, and pictures, alone or in combination, delivered over a packet-switched domain.
IP (Internet Protocol)	The method by which data is sent from one computer to another on the Internet or other networks.

Term or Abbreviation (Expansion)	Definition / Description
ISUP (Integrated Services Digital Network User Part)	A message protocol to support call set up and release for interoffice voice call connections over SS7 Signaling.
LPG (Legacy PSAP Gateway)	The Legacy PSAP Gateway is a signaling and media interconnection point between an ESInet and a legacy PSAP. It plays a role in the delivery of emergency calls that traverse an i3 ESInet to get to a legacy PSAP, as well as in the transfer and alternate routing of emergency calls between legacy PSAPs and NG9-1-1 PSAPs. The Legacy PSAP Gateway supports an IP (i.e., SIP) interface towards the ESInet on one side, and a traditional MF or Enhanced MF interface (comparable to the interface between a traditional Selective Router and a legacy PSAP) on the other.
LRF (Location Retrieval Function)	The IMS-associated functional entity that handles the retrieval of location information for the emergency caller including, when required, interim location information, initial location information, and updated location information. The LRF may interact with a separate RDF or contain an integrated RDF in order to obtain routing information for an emergency call.
LS (Location Server)	General term for the entity responsible for obtaining the location of the User Equipment (UE). See 3GPP TS 23.167. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=799
LSRG (Legacy Selective Router Gateway)	The LSRG provides an interface between a 9-1-1 Selective Router and an ESInet, enabling calls to be routed and/or transferred between Legacy and NG networks. A tool for the transition process from Legacy 9-1-1 to NG9-1-1.
MF (Multi-Frequency)	A type of in-band signaling used on analog interoffice and 9-1-1 trunks.
MGCF (Media Gateway Control Function)	An IMS element that facilitates call control, interfacing the Packet Switched domain to the Circuit Switched domain, when interworking between the IMS and PSTN is required.

Term or Abbreviation (Expansion)	Definition / Description
MGW (Media Gateway)	A translation device that converts media streams between dissimilar telecommunications networks, e.g., to support communications between legacy time-division multiplexing (TDM)-based voice networks and next-generation Internet Protocol (IP)-based voice networks.
MLP (Mobile Location Protocol)	A protocol that may be used for mobile location queries.
MPC/GMLC (Mobile Positioning Center/Gateway Mobile Location Center)	A Functional Entity that provides an interface between the wireless originating network and the Emergency Services Network. The MPC/GMLC retrieves, forwards, stores and controls position data within the location services network. It interfaces with the location server (e.g., Position Determining Entity (PDE)) for initial and updated position determination. The MPC/GMLC restricts access to provide position information only while an emergency call is active.
MSC (Mobile Switching Center)	The wireless equivalent of a Central Office, which provides switching functions for wireless calls.
NANC (North American Numbering Council)	A Federal Advisory Committee that was created to advise the Commission on numbering issues and to make recommendations that foster efficient and impartial number administration.
NANP (North American Numbering Plan)	An integrated telephone numbering plan serving 20 North American countries that share its resources and are in the +1 country code. NANP numbers are ten-digit numbers consisting of a three-digit Numbering Plan Area (NPA) code, commonly called an area code, followed by a seven-digit local number. The format is usually represented as NXX-NXX-XXXX where N is any digit from 2 through 9 and X is any digit from 0 through 9.
NCAS (Non Call Associated Signaling)	A method for delivery of wireless 9-1-1 calls in which the Mobile Directory Number and other call associated data are passed from the Mobile Switching Center to the PSAP outside the voice path. Also known as:

Term or Abbreviation (Expansion)	Definition / Description
	Non Call-path Associated Signaling Non-Call Associated Signaling
NENA (National Emergency Number Association)	NENA is referred to as The 9-1-1 Association, which is fully dedicated to the continued improvement and modernization of the 9-1-1 emergency communication system. NENA's approach includes research, standards development, training, education, certification, outreach, and advocacy through communication with stakeholders. As an ANSI-accredited Standards Developer, NENA works with 9-1-1 professionals, public policy leaders, emergency services and telecommunications industry partners, like-minded public safety associations, and more. Current NENA activities center on awareness, documentation, and implementation for Next Generation 9-1-1 (NG9-1-1) and international three-digit emergency communication systems. NENA's worldwide members join with the emergency response community in striving to protect human life, preserve property, and maintain the security of all communities.
NG9-1-1 (Next Generation 9-1-1)	An IP-based system comprised of hardware, software, data, and operational policies and procedures that: (A) provides standardized interfaces from emergency call and message services to support emergency communications; (B) processes all types of emergency calls, including voice, data, and multimedia information; (C) acquires and integrates additional emergency call data useful to call routing and handling; (D) delivers the emergency calls, messages, and data to the appropriate public safety answering point and other appropriate emergency entities; (E) supports data or video communications needs for coordinated incident response and management. Also known as: Next Generation 9-1-1 Services.

Term or Abbreviation (Expansion)	Definition / Description
NGCS (Next Generation 9-1-1 Core Services)	The set of services needed to process a 9-1-1 call on an ESInet. It includes, but is not limited to, the ESRP, ECRF, LVF, BCF, Bridge, Policy Store, Logging Services, and typical IP services such as DNS and DHCP. The term NG9-1-1 Core Services includes the services and not the network on which they operate. See Emergency Services IP Network.
NOC (Network Operation Center)	A centralized location where a company and their staff can provide supervision 24 hours a day to help monitor and manage a company's services, databases, external services, firewalls, and network.
NPA (Numbering Plan Area)	Encoded numerically with a three-digit telephone number prefix, commonly called the area code. Each telephone is assigned a seven-digit telephone number unique only within its respective plan area. The telephone number consists of a three-digit central office code and a four-digit station number. The combination of an area code and the telephone number serves as a destination routing address in the public switched telephone network (PSTN).
NPD (Numbering Plan Digit)	A component of the traditional 8-digit 9-1-1 signaling protocol between the Enhanced 9-1-1 Control Office and the PSAP CPE. Identifies 1 of 4 possible area codes.
NTWG (Network Working Group)	A Working Group under CISC that undertakes tasks related to the network operations and addresses any other network issues such as mass calling events.
OCIF (Outbound Call Interface Function)	Part of the NGCS responsible for handling calls originating from i3-PSAPs over their serving ESInet/NGCS.
OSP (Originating Service Provider)	A communications provider that allows its users or subscribers to originate 9-1-1 voice or nonvoice messages from the public to public safety answering points, including but not limited to wireline, wireless, and voice over internet protocol service.
pANI (Pseudo Automatic Number Identification)	A telephone number used to support routing of wireless 9-1-1 calls. It may identify a wireless cell, cell sector or

Term or Abbreviation (Expansion)	**Definition / Description**
	PSAP to which the call should be routed. Also known as: Routing Number.
PASSporT (Personal Assertion Token)	A cryptographically signed token to protect the integrity of the identity of the originator and to verify the assertion of the identity information at the destination.
PCA (PSAP Credentialing Agency)	The root authority designated to issue and revoke security credentials (in the form of an X.509 certificate) to authorized 9-1-1 agencies in an i3-compliant infrastructure.
P-CSCF (Proxy Call Session Control Function)	The P-CSCF is the first contact point for the user equipment (UE) within the IMS core network. For an IMS-based emergency call, the P-CSCF detects the emergency call and forwards it to an E-CSCF.
PIDF-LO (Presence Information Data Format - Location Object)	Provides a flexible and versatile means to represent location information in a SIP header using an XML schema.
PSAP (Public Safety Answering Point)	Public Safety Answering Point (PSAP): A physical or virtual entity where 9-1-1 calls are delivered by the 9-1-1 Service Provider. • Primary PSAP: A PSAP to which 9-1-1 calls are routed directly from the 9-1-1 Control Office. • Secondary PSAP: A PSAP to which 9-1-1 calls are transferred from a Primary PSAP. • Alternate PSAP: A PSAP designated to receive calls when the primary PSAP is unable to do so. • Consolidated PSAP: A facility where multiple Public Safety Agencies choose to operate as a single 9-1-1 entity. • Legacy PSAP: A PSAP that cannot process calls received via i3-defined call interfaces (IP-based calls) and still requires the use of CAMA or ISDN trunk technology for delivery of 9-1-1 emergency calls.

Term or Abbreviation (Expansion)	**Definition / Description**
	• Serving PSAP: The PSAP to which a call would normally be routed. • NG9-1-1 PSAP: This term is used to denote a PSAP capable of processing calls and accessing data services as defined in NENA's i3 specification, NENA-STA-010, and referred to therein as an "i3 PSAP." • Virtual PSAP: An operational model directly enabled through NG9-1-1 features and/or network hosted PSAP equipment in which telecommunicators are geographically dispersed, rather than working from the same physical location. Remote access to the PSAP applications by the dispersed telecommunicators requires the appropriate network connections, security, and work station equipment at the remote location. The virtual work place may be a logical combination of physical PSAPs, or an alternate work environment such as a satellite facility, or any combination of the above. Workers are connected and interoperate via IP connectivity.
PSTN (Public Switched Telephone Network)	The network of equipment, lines, and controls assembled to establish communication paths between calling and called parties in North America.
RDF (Routing Determination Function)	The IMS-associated functional entity, which may be integrated in a Location Server (e.g., GMLC) or in an LRF, and provides the proper outgoing address to the E-CSCF for routing the emergency request towards a PSAP. It can interact with a location functional entity (e.g., GMLC) to manage ESQK allocation and management and deliver location information to the PSAP.
RPH (Resource-Priority Header)	A header field used on SIP calls to indicate priority that proxy servers give to specific calls. The Resource-Priority

Term or Abbreviation (Expansion)	Definition / Description
	header field does not indicate that a call is an emergency call (see Request-URI).
SHAKEN (Signature-based Handling of Asserted Information Using toKENs)	An industry framework for managing the deployment of Secure Telephone Identity (STI) technologies with the purpose of providing end-to-end cryptographic authentication and verification of the telephone identity and other information in an Internet Protocol (IP)-based service provider voice network. See ATIS-1000074 [11].
SIP (Session Initiation Protocol)	A protocol specified by the IETF (RFC 3261) that defines a method for establishing multimedia sessions over the Internet. Used as the call signaling protocol in VoIP, NENA i2, and NENA i3.
SOP (Standard Operating Procedure)	A written directive that provides a guideline for carrying out an activity. The guideline may be made mandatory by including terms such as "shall" rather than "should" or "must" rather than "may."
SR (Selective Router)	The Central Office that provides the tandem switching of 9-1-1 calls. It controls delivery of the voice call with ANI to the PSAP and provides Selective Routing, Speed Calling, Selective Transfer, Fixed Transfer, and certain maintenance functions for each PSAP. Also known as Enhanced 9-1-1 Control Office.
SRDB (Selective Routing Database)	The routing table that contains telephone number to ESN relationships which determines the routing of 9-1-1 calls.
SS7 (Signaling System No. 7)	An out-of-band signaling system used to provide basic routing information, call set-up and other call termination functions. Signaling is removed from the voice channel itself and put on a separate data network. Also known as CCS7 (Common Channel Signaling No. 7).
STI-CPS (Secure Telephone Identity Call Placement Service)	A service consisting of one or more logical components that receives PASSporTs published by one service provider, for retrieval by another service provider.

Term or Abbreviation (Expansion)	Definition / Description
STIR (Secure Telephone Identity Revisited)	SIP header-based mechanism for verification that the originator of a SIP session is authorized to use the claimed source telephone number, where session is established with SIP end to end.
TCPA (Telephone Consumer Protection and Truth in Caller ID Act)	An Act that prohibits the knowing transmittal of "misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value."
TDM (Time Division Multiplexing)	A digital multiplexing technique for combining a number of signals into a single transmission facility by interweaving pieces from each source into separate time slots. TDM is a predecessor to IP signaling.
TDoS (Telephony Denial of Service)	A form of DoS directed at a telephony interface which generates numerous phone calls, tying up the network and preventing the destination from receiving legitimate calls. Occasionally the "T" in TDoS may be shown as Telephone or Telecommunications.
TN (Telephone Number)	A sequence of digits assigned to a device to facilitate communications via the public switched telephone network or other private network.
TRACED (Telephone Robocall Abuse Criminal Enforcement and Deterrence)	An Act signed into law in December 2019 that provides tools to discourage illegal robocalls, protect consumers, and crack down on offenders.
TSP (Telecommunications Service Provider)	A business that provides voice or data transmission services. These services are provided over a telecommunications network that transmits any combination of voice, video and/or data between users. A TSP could be, but is not limited to, a Local Exchange Carrier (LEC), a wireless telecommunications provider, a Commercial Mobile Radio Service provider, or a PBX service provider.
UE (User Equipment)	A device allowing a user access to network services.
URI (Uniform Resource Identifier)	An identifier consisting of a sequence of characters matching the syntax rule that is named <URI> in RFC

Term or Abbreviation (Expansion)	Definition / Description
	3986. It enables uniform identification of resources via a set of naming schemes. A URI can be further classified as a locator, a name, or both. The term "Uniform Resource Locator" (URL) refers to the subset of URIs that, in addition to identifying a resource, provides a means of locating the resource by describing its primary access mechanism (e.g., its network "location"). The term "Uniform Resource Name" (URN) has been used historically to refer to both URIs under the "urn" scheme [RFC2141], which are required to remain globally unique and persistent even when the resource ceases to exist or becomes unavailable, and to any other URI with the properties of a name. An example of a URI that is neither a URL nor a URN is sip:psap@example.com.
URN (Uniform Resource Name)	A URN is a type of URI. Uniform Resource Names (URNs) are intended to serve as persistent, location-independent, resource identifiers and are designed to make it easy to map other namespaces (which share the properties of URNs) into URN-space. An example of a URN is urn:service.sos.
VoIP (Voice over Internet Protocol)	Technology that permits delivery of voice calls and other real-time multimedia sessions over IP networks.
VPC (VoIP Positioning Center)	The element that provides routing information to support the routing of VoIP emergency calls, and cooperates in delivering location information to the PSAP over the existing ALI DB infrastructure.
WCM (Wireline Compatibility Mode)	A wireless 9-1-1 signaling arrangement in which an ESRK (Emergency Services Routing Key) is sent as the ANI (Automatic Number Identification) over dedicated trunks to the Selective Router.
WG (Working Group)	A group of people formed to discuss and develop a response to a particular issue. Working Groups (WGs) are the primary mechanism for development of IETF specifications and guidelines, many of which are intended to be standards or recommendations.

12 References

[1] National Emergency Number Association. "NENA Knowledge Base Glossary." Updated August 31, 2023. https://kb.nena.org/wiki/Category:Glossary.

[2] Telephone Consumer Protection Act of 1991. P.L. 102-243, 47 U.S.C. §227.

[3] Federal Communications Commission. *Notice of Inquiry In the Matter of Call Authentication Trust Anchor*, WC Docket No. 17-97. FCC 17-89. Adopted July 13, 2017.

[4] Federal Communications Commission. *Declaratory Ruling and Third Further Notice of Proposed Rulemaking In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls (CG Docket No. 17-59) and Call Authentication Trust Anchor (WC Docket No. 17-97).* FCC 19-51. Adopted June 6, 2019.

[5] Federal Communications Commission. *Report and Order and Further Notice of Proposed Rulemaking In the Matter of Call Authentication Trust Anchor (WC Docket 17-97) and Implementation of TRACED Act Section 6(a)—Knowledge of Customers by Entities with Access to Numbering Resources (WC Docket No. 20-67)*. FCC 20-42. Adopted March 31, 2020.

[6] Truth in Caller ID Act of 2009. Pub. L. No. 111–331, 47 U.S.C. §227.

[7] Federal Communications Commission. *Truth in Caller ID Rules*. 47 CFR Part 64, (WC Docket Nos. 18–335, 11–39; FCC 19–73). 84 FR 45669. Effective 2/5/2020.

[8] Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act. Pub. L. 116-105. December 30, 2019.

[9] Federal Communications Commission. *Second Report and Order In the Matter of Call Authentication Trust Anchor (WC Docket 17-97)*. FCC 20-136. Adopted September 29, 2020.

[10] Internet Engineering Task Force. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk. RFC 5280, May 2008.

[11] Alliance for Telecommunications Industry Solutions. *ATIS Standard on Signature-based Handling of Asserted information using toKENs (SHAKEN)*. ATIS-1000074.v002. Washington, DC: ATIS, July 2021.

[12] National Emergency Number Association. *NENA i3 Standard for Next Generation 9-1-1*. NENA-STA-010.3-2021. Alexandria, VA: NENA, approved July 12, 2021.

[13] Telecommunications Industry Association and Alliance for Telecommunications Industry Solutions. *Enhanced Wireless 9-1-1 Phase 2*. Washington, DC: ATIS J-STD-036-C-2. Washington, DC: ATIS, June 2017.

[14] Federal Communications Commission. *Task Force on Optimal PSAP Architecture (TFOPA) Working Group 1 Report on Optimal Cybersecurity Approach for PSAPs*. December 10, 2015.

[15] National Emergency Number Association. *NENA Security for Next-Generation 9-1-1 Standard (NG-SEC)*. NENA-STA-040.2-202Y (originally 75-001, v1). Alexandria, VA: NENA (forthcoming).

[16] National Emergency Number Association. *NENA Standard for the Implementation of the Wireless Emergency Service Protocol E2*. NENA-STA-018.2-2021 (originally 05-001). Alexandria, VA: NENA, approved February 17, 2021.

[17] National Emergency Number Association. *NENA Standard Data Formats for E9-1-1 Data Exchange & GIS Mapping*. NENA-STA-015.10-2018 (Originally 02-010). Alexandria, VA: NENA, approved August 12, 2018.

[18] National Emergency Number Association. *NENA ALI Query Service Standard*. NENA 04-005. Alexandria, VA: NENA, Issue 1, November 21, 2006.

[19] Alliance for Telecommunications Industry Solutions. *Signature-based Handling of Asserted information using toKENs (SHAKEN): Out-of-Band PASSporT Transmission Involving TDM Networks*. ATIS-1000096. Washington, DC: ATIS, July 2021.

[20] Alliance for Telecommunications Industry Solutions. *Extending STIR/SHAKEN Over TDM)*. ATIS-1000095. Washington, DC: ATIS, July 2021.

[21] Alliance for Telecommunications Industry Solutions. *Emergency Calling Service*. ATIS-1000628.2000(S2020). Washington, DC: ATIS, May 2000.

[22] Alliance for Telecommunications Industry Solutions. *Signature-based Handling of Asserted information using toKENs (SHAKEN): Governance Model and Certificate Management*. ATIS-1000080.v005. Washington, DC: ATIS, December 2022.

[23] Federal Communications Commission. *Sixth Report and Order In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls (CG Docket No. 17-59), Fifth Report and Order In the Matter of Call Authentication Trust Anchor (WC Docket No. 17-97), Order on Reconsideration In the Matter of Call Authentication Trust Anchor (WC Docket No. 17-97), Seventh Further Notice of Proposed Rulemaking In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls (CG Docket No. 17-59), and Fifth Further Notice of Proposed Rulemaking In the Matter of Call Authentication Trust Anchor (WC Docket No. 17-97)*. FCC 22-37. Adopted May 19, 2022.

[24] Alliance for Telecommunications Industry Solutions. *Analysis of Non-IP Call Authentication Mechanisms in Support of Emergency Services*. ATIS-0500046. Washington, DC: ATIS, March 2022.

ACKNOWLEDGEMENTS

The National Emergency Number Association (NENA) Spoofing Mitigation Working Group under the 9-1-1 Core Services Committee developed this document.

NENA recognizes the following industry experts and their employers for their contributions to the development of this document.

Members	Employer
Amy McDowell, ENP, Committee Co-Chair	Greenville County, SC
Diane Harris, ENP, Committee Co-Chair	Zetron, Inc.
Terry Reese, Working Group Chair	Ericsson, Inc.
David Beckerley, ENP	City of Austin, TX
Fae Black	Synergem Technologies, Inc.
Tom Breen, ENP	SecuLore, an Exacom company
Terri Brooks	T-Mobile USA, Inc.
Kirk Burroughs	Apple
Victor Burton	Comtech
John Eon	Consolidated Communications Inc.
Michael Fain	Mission Critical Partners, LLC
Tom Hsu	Nokia
Travis LePage, ENP	Federal Engineering, Inc.
Robert Little	City of Columbus, OH
Roger Marshall	Comtech
Alan McClellan, ENP	Washington County, TN
Glen Milligan	Niagara Regional Police Service ON
Dan Mongrain	Motorola Solutions, Inc.
Peter Musgrove	AT&T
Richard Polishak	TELUS
Aleisha Rucker-Wright	Georgia Emergency Communications Authority
Jeff Torres	Verizon Wireless
Steve Walsh	Washington State 911 Coordination Office
Jason Wellonen	Carbyne, Inc.
Allenna Wiggins, ENP, RPL	Alameda County Sheriff

Special Acknowledgements:

Sandy Dyre, ENP, Committee Resource Manager, has facilitated the production of this document through the prescribed approval process.

The Spoofing Mitigation Working Group is part of the NENA Development Group that is led by:

- Wendi Rooney, ENP, and Lisa Dodson, ENP, Development Steering Council Co-Chairs
- Brandon Abley, ENP, Chief Technology Officer
- April Heinze, ENP, VP, Chief of 9-1-1 Operations