ATIS-1000098

Session Initiation Protocol (SIP) Resource-Priority Header (RPH) and Priority Header Signing in Support of Emergency Calling

JOINT STANDARD

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

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

The SIP Forum is a leading IP communications industry association that engages in numerous activities that promote and advance SIP-based technology, such as the development of industry recommendations; interoperability testing events and special workshops, educational activities, and general promotion of IP communications standards, services, and technology for service provider, enterprise, and governmental applications. The SIP Forum is also the producer of the annual SIPNOC conferences (for SIP Network Operators Conference), focused on the technical requirements of the service provider community. One of the Forum's technical activities is the development of the SIPconnect Technical Recommendation – a standards-based SIP trunking recommendation that provides detailed guidelines for direct IP peering and interoperability between IP PBXs and SIP-based service provider networks, and the SIPconnect Certification Testing Program, a unique certification testing program that includes a certification test suite and test platform, and an associated "SIPconnect Certified" logo program that provides an official "seal of certification" for companies products and services that have officially achieved conformance with the SIPconnect specification. Other important Forum initiatives include work in security, SIP and IPv6, and IP-based Network-to-Network Interconnection (IP-NNI). For more information about all SIP Forum initiatives, please visit:

< http://www.sipforum.org/ >

Notice of Disclaimer & Limitation of Liability

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

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

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

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

Is an ATIS & SIP Forum Joint Standard developed by the **ATIS/SIP Forum IP-NNI Task Force** under the **ATIS Packet Technologies and Systems Committee (PTSC)** and the **Technical Working Group (TWG)** under the **SIP Forum**.

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

SIP Forum LLC
733 Turnpike Street, Suite 192
North Andover, MA 01845

ATIS-1000098

ATIS Standard on

Session Initiation Protocol (SIP) Resource-Priority Header (RPH) and Priority Header Signing in Support of Emergency Calling

Alliance for Telecommunications Industry Solutions

Approved July 12, 2021

Abstract

This standard defines how the IETF Personal Assertion Token (PASSporT) Extension for Resource-Priority Authorization [IETF RFC 8443, *PASSporT Extension for Resource-Priority Authorization*], with the extensions defined in RFC 9027, *Assertion Values for Resource Priority Header and SIP Priority Header Claims in Support of Emergency Services Networks*, and the associated STIR mechanisms, are used to sign the Session Initiation Protocol (SIP) Resource-Priority Header (RPH) field and convey assertions of Resource-Priority associated with an emergency call or callback call. This standard also addresses the signing of the SIP Priority header field associated with callback calls. Specifically, this standard describes a procedure for providing cryptographic authentication and verification of the information in the SIP RPH field and SIP Priority header field in Internet Protocol (IP)-based service provider communication networks in support of emergency calling.

Foreword

The Alliance for Telecommunications Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The Packet Technologies and Systems Committee (PTSC) develops and recommends standards and technical reports related to services, architectures, and signaling, in addition to related subjects under consideration in other North American and international standards bodies. PTSC coordinates and develops standards and technical reports relevant to telecommunications networks in the U.S., reviews and prepares contributions on such matters for submission to U.S. International Telecommunication Union Telecommunication Sector (ITU-T) and U.S. ITU Radiocommunication Sector (ITU-R) Study Groups or other standards organizations, and reviews for acceptability or per contra the positions of other countries in related standards development and takes or recommends appropriate actions.

The SIP Forum is an IP communications industry association that engages in numerous activities that promote and advance SIP-based technology, such as the development of industry recommendations, the SIPit, SIPconnect-IT, and RTCWeb-it interoperability testing events, special workshops, educational seminars, and general promotion of SIP in the industry. The SIP Forum is also the producer of the annual SIP Network Operators Conference (SIPNOC), focused on the technical requirements of the service provider community. One of the Forum's notable technical activities is the development of the SIPconnect Technical Recommendation – a standards-based SIP trunking recommendation for direct IP peering and interoperability between IP Private Branch Exchanges (PBXs) and SIP-based service provider networks. Other important Forum initiatives include work in Video Relay Service (VRS) interoperability, security, Network-to-Network Interoperability (NNI), and SIP and IPv6.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, PTSC, 1200 G Street NW, Suite 500, Washington, DC 20005, and/or to the SIP Forum, 733 Turnpike Street, Suite 192, North Andover, MA, 01845.

The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages. The word *may* denotes an optional capability that could augment the standard. The standard is fully functional without the incorporation of this optional capability.

The **ATIS/SIP Forum IP-NNI Task Force** under the **ATIS Packet Technologies and Systems Committee (PTSC)** and the **SIP Forum Technical Working Group (TWG)** was responsible for the development of this document.

Table of Contents

Table of Figures

ATIS Standard on –

Session Initiation Protocol (SIP) Resource-Priority Header (RPH) and Priority Header Signing in Support of Emergency Calling

1 Scope & Purpose

1.1 Scope

As specified in IETF RFC 4412, *Communications Resource Priority for the Session Initiation Protocol (SIP)*, the Session Initiation Protocol (SIP) Resource-Priority Header (RPH) field may be used by SIP user agents, including Public Switched Telephone Network (PSTN) gateways and terminals, and SIP proxy servers to influence prioritization afforded to communication sessions, including PSTN calls. As discussed in 3GPP TS 24.229, *Technical Specification Group Services and System Aspects; IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3*, where the network has a requirement to prioritize emergency calls, it can use the "esnet" namespace in the Resource-Priority Header field (as defined in IETF RFC 7135, *Registering a SIP Resource Priority Header Field Namespace for Local Emergency Communications*, to do so. Where the Resource-Priority Header field is used for this purpose, it is inserted by the entity identifying the emergency call, i.e., the Proxy Call Session Control Function (P-CSCF) or the Interconnection Border Control Function (IBCF). There is no usage of this namespace from the User Agent (UA), and when this namespace is used, the trust domain implementation removes it if set by the UA.

After an emergency call is received by a Public Safety Answering Point (PSAP), it is sometimes necessary for the call taker to call the emergency caller back (e.g., if the caller disconnects prematurely). IETF RFC 7090, *Public Safety Answering Point (PSAP) Callback*, describes the use of the SIP Priority header field, with the value "psap-callback" to mark such calls to allow special network handling of the call, such as bypassing services that might preclude the call from completing. There is no protection against misuse of the SIP Priority field, and because, as IETF RFC 7090 [Ref 10] illustrates, the SIP Priority header field may affect routing, it is desirable to protect it from modification.

Like caller identity information associated with emergency calls and callback calls, the SIP RPH and Priority header fields could also be spoofed by unauthorized entities, impacting Public Safety communications and emergency response. Next Generation 9-1-1 (NG9-1-1) Emergency Services Networks receiving SIP RPHs across Internet Protocol Network-to-Network Interfaces (IP NNIs) from Internet Protocol (IP) originating networks cannot easily determine whether the SIP RPH was populated by an authorized Originating Service Provider or by an unauthorized entity. Likewise, the home network of an emergency caller cannot determine whether the SIP Priority header associated with a callback call was populated by an authorized party and can be trusted.

This ATIS standard leverages the Signature-based Handling of Asserted information using toKENs (SHAKEN) model specified in ATIS-1000074-E, *Errata on ATIS Standard on Signature-based Handling of Asserted information using toKENs (SHAKEN)*, to cryptographically sign and verify the SIP RPH and Priority header fields associated with emergency calls and callback calls using the Personal Assertion Token (PASSporT) extension defined in IETF RFC 8443 [Ref 16] with the assertion values described in RFC 9027 [Ref 7] and the associated Secure Telephone Identity (STI) protocols described in 3GPP TS 24.229 [Ref 2]. Note that application of SIP RPH signing to emergency calls and SIP RPH and Priority header signing to callback calls is in addition to the caller identity authentication and verification defined in ATIS-1000074-E [Ref 5].

This ATIS standard is intended to provide a framework and guidance on how to use the PASSporT extension defined in IETF RFC 8443 [Ref 16], with the RPH assertion values and SIP Priority header claim specified in RFC 9027 [Ref 07] and the associated STI protocols to cryptographically sign and verify the SIP RPH and Priority header values associated with emergency calls or callback calls that cross IP NNI boundaries.

The scope of this ATIS standard is limited to the cryptographic signing and verifying of SIP RPH and Priority header field contents associated with emergency and callback calls (i.e., RPH values in the "esnet" namespace and a

Priority header value of "psap-callback"). This standard does not address caller identity (SHAKEN) authentication and verification associated with emergency calls and callback calls, except in the context of call flow descriptions, nor does it discuss specific impacts to call processing or routing procedures associated with the use of the Priority header to mark callback calls. Finally, the display of information associated with the verification of SIP RPH and Priority header values is outside the scope of this document.

1.2 Purpose

Illegitimate spoofing of SIP RPH values in the "esnet" namespace in the signaling associated with emergency calls and callback calls is a concern for Public Safety. NG9-1-1 System Service Providers will interconnect with multiple Originating Service Providers and will benefit from knowing whether the SIP RPH value received in incoming signaling can be trusted. Likewise, home network providers serving emergency callers will benefit from knowing whether the Priority header accompanying a callback call can be trusted before applying special processing or routing to such calls. The purpose of this standard is to provide a framework for cryptographically signing the SIP RPH and Priority header fields and verifying that the SIP RPH and Priority header fields can be trusted to mitigate against unauthorized spoofing of, or tampering with, the information conveyed in the SIP RPH or Priority header. This framework will leverage the SHAKEN infrastructure for caller identity authentication and verification and will describe how the PASSporT "rph" extension defined in IETF RFC 8443 [Ref 16], with the RPH assertion values and SIP Priority header claim described in RFC 9027 [Ref 7], can be used for the purpose of providing a trust mechanism for the SIP RPH associated with emergency calls and the SIP RPH and Priority header associated with callback calls that cross IP NNI boundaries.

2 Normative References

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

[Ref 1] 3GPP TS 23.228, *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2.3.*[1]

[Ref 2] 3GPP TS 24.229, *Technical Specification Group Services and System Aspects; IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3.* [1]

[Ref 3] ATIS-0500032, *ATIS Standard for Implementation of an IMS-based NG9-1-1 Service Architecture*.[2]

[Ref 4] ATIS-0700015.v004, *ATIS Standard for Implementation of 3GPP Common IMS Emergency Procedures for IMS Origination and ESInet/Legacy Selective Router Termination*.[2]

[Ref 5] ATIS-1000074-E, *Errata on ATIS Standard on Signature-based Handling of Asserted information using toKENs (SHAKEN).* [2]

[Ref 6] ATIS-1000082, *Technical Report on SHAKEN APIs for a Centralized and Signature Validation Server*.[2]

[Ref 7] IETF RFC 9027, *Assertion Values for Resource Priority Header and SIP Priority Header Claims in Support of Emergency Services Networks.*[3]

[Ref 8] IETF RFC 4412, *Communications Resource Priority for the Session Initiation Protocol (SIP).*[3]

[Ref 9] IETF RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.[3]

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

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

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

[Ref 10] IETF RFC 7090, *Public Safety Answering Point (PSAP) Callback*.[3]

[Ref 11] IETF RFC 7135, *Registering a SIP Resource Priority Header Field Namespace for Local Emergency Communications*.[3]

[Ref 12] IETF RFC 7230, *Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing*.[3]

[Ref 13] IETF RFC 8224, *Authenticated Identity Management in the Session Initiation Protocol.*[3]

[Ref 14] IETF RFC 8225, PASSporT: *Personal Assertion Token.*[3]

[Ref 15] IETF RFC 8226, *Secure Telephone Identity Credentials: Certificates.*[3]

[Ref 16] IETF RFC 8443, *PASSporT Extension for Resource-Priority Authorization*.[3]

3 Definitions, Acronyms, & Abbreviations

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

3.1 Definitions

Callback Call: A request whose purpose is to reconnect with the party that originated an emergency call.

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

Next Generation 9-1-1 (NG9-1-1): An IP-based system comprised of managed IP-based networks (e.g., ESInets), functional elements (applications), and databases that replicate traditional E9-1-1 features and functions, and provide additional capabilities. NG9-1-1 is designed to provide access to emergency services from all connected communications sources, and provide multimedia data capabilities for Public Safety Answering Points (PSAPs) and other emergency service organizations.

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

Priority Header: A SIP header field that is used to mark callback calls to increase the chances of reaching the emergency caller by allowing networks to use that marking to apply preferential treatment to those calls. See IETF RFC 7090 [Ref 10] for further details.

3.2 Acronyms & Abbreviations

3GPP	3rd Generation Partnership Project
ATIS	Alliance for Telecommunications Industry Solutions
CRL	Certificate Revocation List
CSCF	Call Session Control Function
CVT	Call Validation Treatment
E-CSCF	Emergency Call Session Control Function
ESInet	Emergency Services IP Network
ESRP	Emergency Service Routing Proxy
HTTP	Hypertext Transfer Protocol

HTTPS	Hypertext Transfer Protocol Secure
IBCF	Interconnection Border Control Function
I-CSCF	Interrogating Call Session Control Function
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IP NNI	Internet Protocol Network-to-Network Interface
JSON	JavaScript Object Notation
LRF	Location Retrieval Function
NG9-1-1	Next Generation 9-1-1
NNI	Network-to-Network Interface
PASSporT	Personal Assertion Token
P-CSCF	Proxy Call Session Control Function
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
RDF	Routing Determination Function
RPH	Resource-Priority Header
SHAKEN	Signature-based Handling of Asserted information using toKENs
SIP	Session Initiation Protocol
SKS	Secure Key Store
STI	Secure Telephone Identity
STI-AS	Secure Telephone Identity Authentication Service
STI-CA	Secure Telephone Identity Certification Authority
STI-CR	Secure Telephone Identity Certificate Repository
STI-VS	Secure Telephone Identity Verification Service
STIR	Secure Telephone Identity Revisited
TN	Telephone Number
UA	User Agent
URI	Uniform Resource Identifier

4 Assumptions

4.1 General Assumptions

This standard makes the following assumptions regarding the application of RPH signing to emergency calls and callback calls:

1. A Resource-Priority Header (RPH) in the "esnet" namespace may or may not be associated with an emergency origination by the P-CSCF in the originating IMS network, based on local policy.
2. Caller identity assertion/authentication and/or RPH signing will be performed by the originating network after it has been determined that the emergency call is to be routed to an NG9-1-1 Emergency Services Network.
3. The NG9-1-1 Emergency Services Network will be responsible for performing verification of PASSporT information received with an emergency call.
4. Callback calls routed via the NG9-1-1 Emergency Services Network will be marked as "psap-callback" and will contain an RPH with a value of "esnet.0".
5. The NG9-1-1 Emergency Services Network will be responsible for performing caller identity attestation/authentication and RPH and SIP Priority header signing on callback calls.
6. Verification of a signed caller identity/RPH/Priority header will be performed by the terminating home network for the callback call.
7. A Service Provider can use the same Secure Telephone Identity (STI) certificates for signing a SIP RPH/Priority header as they use for telephone number (TN) signing, but is not required to do so.
8. SIP RPH signing does not change or modify 9-1-1/callback call processing, signaling and routing procedures; it simply provides a security tool for transit and receiving providers to determine if the SIP RPH can be trusted.
9. If validation of the signed caller identity or SIP RPH associated with a 9-1-1 origination fails, the 9-1-1 call will be delivered to the PSAP with caller identity and SIP RPH, as well as the results of the caller identity and RPH verification.
10. If validation of the signed caller identity or SIP RPH/Priority header associated with a callback call fails, terminating Service Provider local policy will determine call processing, such as whether the call should be delivered with caller identity and/or SIP RPH/Priority header information intact. Note that if the call proceeds, verification status information will be included in the associated SIP signaling.
11. Signing of caller identity is separate from SIP RPH/Priority header signing. Separate SIP Identity headers are used for SIP RPH/Priority header signing and caller identity signing.

4.2 Architectural Assumptions

In keeping with the SHAKEN reference architecture described in ATIS-1000074-E [Ref 5], which shows a Call Session Control Function (CSCF) interacting with a Secure Telephone Identity Authentication Service (STI-AS) (in the originating network) and a Secure Telephone Identity Verification Service (STI-VS) (in the terminating network), initial discussions related to the architecture to support the application of SHAKEN to 9-1-1 assumed that, for 9-1-1 originations, the Emergency Call Session Control Function (E-CSCF) in the originating IMS network would interact with the STI-AS, and an E-CSCF (in an IMS-based NG9-1-1 Emergency Services Network) or an i3 Emergency Service Routing Proxy (ESRP) (in an i3 NG9-1-1 Emergency Services Network) would interact with the STI-VS. However, there is currently no reference point defined in 3GPP standards that supports interactions between an E-CSCF and an Application Server. 3GPP TS 23.228, *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2.3*, and 3GPP TS 24.229 [Ref 2] do, however, describe the use of the Ms reference point between an IBCF and an Application Server over which HTTP 1.1, as specified in IETF RFC 7230, *Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing*, is currently defined. Specifically, Annex V of 3GPP TS 24.229 [Ref 2] defines a signingRequest/signingResponse and verificationRequest/verificationResponse to support caller identity signing and verification. Note that this mechanism is also supported by ATIS-1000082, *Technical Report on SHAKEN APIs for a Centralized and Signature Validation Server*, where the exit IBCF in the originating network is the "Authenticator" and the entry IBCF in the IMS NG9-1-1 Emergency Services Network is the "Verifier".

Based on 3GPP TS 24.229 [Ref 2], to get an asserted identity signed, the client sends an HTTP POST request towards the signing server containing a PASSporT SHAKEN object. As currently defined, the signingRequest includes "orig" and "dest" claims, "iat", and "origid". The signingRequest may also include an "attest" parameter that identifies the relation between the service provider attesting the identity and the subscriber. (According to 3GPP TS 24.229 [Ref 2], the signingRequest may also include a "div" claim identifying the diverting user, if applicable.) The ability for an IBCF to include this information in a signingRequest sent to an STI-AS has other architectural implications. Specifically, it suggests the need for an upstream element, such as a P-CSCF, in the case of an emergency origination, to provide attestation information associated with the caller identity, and to convey the attestation level in the SIP signaling (e.g., in an Attestation-Info header) sent to an exit IBCF. According to 3GPP TS 24.229 [Ref 2] and ATIS-1000082 [Ref 6], upon receiving an HTTP 200 (OK) response to the signingRequest, the IBCF (Authenticator) will include the signingRequest response data in an Identity header field in the forwarded SIP request. This model differs from the framework architecture example described in ATIS-1000074-E [Ref 5], where the SIP INVITE is forwarded by a CSCF to the STI-AS and the STI-AS is responsible for attestation, as well as creating and adding an Identity header field to the request. The reference architecture described in Clause 5.3.1 and flow described in Clause 5.4.1 of this standard illustrate the use of the Ms reference point to support caller identity, as well as RPH signing associated with emergency originations. The IBCF procedures described in Clause 6.1 of this standard also assume the use of the Ms reference point between the IBCF and the STI-AS/STI-VS to support caller identity and RPH signing/verification.

The architecture described in this document to support the application of SHAKEN procedures to callback calls assumes that multimedia callback calls are routed via a Transit Function in an IMS NG9-1-1 Emergency Services Network. The Transit Function is assumed to interact with the STI-AS to support caller identity authentication and signing, as well as RPH/SIP Priority header signing. The Transit Function will invoke the STI-AS for callback calls presented to it after call processing has completed, that is, after the destination interconnected network has been determined. The STI-AS is responsible for asserting/signing the telephone identity of the caller (i.e., the PSAP originating the callback call), as well as the RPH/SIP Priority header values included in the SIP INVITE message associated with the callback call. The STI-AS will return two SIP Identity header fields (one associated with the caller identity and one associated with the RPH/SIP Priority header) to the Transit Function, constructed per IETF RFC 8224, *Authenticated Identity Management in the Session Initiation Protocol*. The Transit Function will include the Identity headers in outgoing signaling and route the callback call towards the home network of the emergency caller. (See ATIS-0500032, *ATIS Standard for Implementation of an IMS-based NG9-1-1 Service Architecture*, for further details related to the processing of callback calls within an IMS NG9-1-1 Emergency Services Network.)

The callback architecture described in this document also assumes that an entry IBCF in the emergency caller’s home network will interact with the STI-VS to support verification of the signed caller identity and RPH/SIP Priority header. As further assumed and described in Clause 6.1.1, the entry IBCF in the emergency caller’s home network will build and send a verificationRequest to the STI-VS over the Ms reference point in an HTTP POST message. The STI-VS will respond by returning a verificationResponse in an HTTP 200 (OK) message that contains a "verstatValue" parameter reflecting the verification status of the Identity header associated with calling identity and a "verstatPriority" parameter reflecting the verification status of the Identity header associated with the RPH/SIP Priority header. The IBCF shall include the verification status information in the SIP signaling sent towards the emergency caller.

While this document assumes an architecture that uses the Ms reference point to support the application of SHAKEN authentication and verification to 9-1-1 originations and callback calls, other architectures are possible.

5 SIP RPH and Priority Header Authentication for 9-1-1

In addition to caller identity authentication/verification, 9-1-1 calls and callback calls may also be subject to RPH signing and, in the case of callback calls, SIP Priority header signing. In the context of 9-1-1 calls, a signed RPH received in an incoming SIP INVITE message will convey to an NG9-1-1 Emergency Services Network provider that they can trust that the RPH was populated by the Originating Service Provider, as opposed to being inserted by a threat agent. In the context of callback calls, a signed RPH and SIP Priority header would indicate that the NG9-1-1 Emergency Services Network provider asserts that they recognize the call is a callback call and, as such, that an RPH value in the "esnet" namespace and a SIP Priority header with the value "psap-callback" are appropriate. The SHAKEN model specified in ATIS-1000074-E [Ref 5] can be leveraged to cryptographically sign and verify the SIP RPH field in SIP INVITE messages associated with 9-1-1 and callback calls and the SIP Priority header associated with callback calls. Using the PASSporT extension defined in IETF RFC 8443 [Ref 16], the RPH assertion values and SIP Priority header claim described in RFC 9027 [Ref 7] and the associated STI protocols, SIP RPH and Priority header field contents can be signed and verified.

The framework specified in this standard supports a trust mechanism for SIP RPH values associated with emergency calls and callback calls, and SIP Priority header values associated with callback calls, crossing IP NNI boundaries. A high-level description of the RPH/SIP Priority header signing flow supported by the framework specified in this standard is as follows:

For emergency calls:

1. The Originating Service Provider cryptographically signs the SIP RPH if present in the SIP INVITE associated with an emergency (9-1-1) origination before sending the call across an IP NNI boundary.
2. The NG9-1-1 System Service Provider verifies the received signed PASSporT for the SIP RPH.

For callback calls:

1. The NG9-1-1 System Service Provider cryptographically signs the SIP RPH and Priority headers associated with a callback call from a PSAP before sending the call across an IP NNI boundary to/towards the emergency caller's home network.
2. The emergency caller's home Service Provider verifies the received signed PASSporT for the SIP RPH/Priority header.

5.1 Protocol Support

This ATIS standard uses the PASSporT "rph" extension specified in IETF RFC 8443 [Ref 16], the RPH assertion values described in RFC 9027 [Ref 7], and associated STI protocols for cryptographic signing of the SIP RPH field in support of emergency service calls. Similarly, this ATIS standard uses the PASSporT "rph" extension specified in IETF RFC 8443 [Ref 16], the RPH assertion values and SIP Priority header claim described in RFC 9027 [Ref 7], and associated STI protocols for cryptographic signing of the SIP RPH/Priority header fields in support of callback calls.

5.1.1 RFC 8225: PASSporT: Personal Assertion Token

IETF RFC 8225, PASSporT: *Personal Assertion Token* [Ref 14], defines a token-based signature that combines the use of JavaScript Object Notation (JSON) Web Tokens, JSON Web Signatures, and X.509 certificate key pairs, or Public Key Infrastructure, to create a trusted signature. The authorized owner of the certificate used to generate the signature can be validated and traced back to the known trust anchor who signed the certificate. The PASSporT includes a number of claims the signer of the token is asserting. The associated public certificate is used to verify the digital signature and the claims included in the PASSporT. The public certificate is also used to validate the entity that signed the token, as defined in IETF RFC 8226, *Secure Telephone Identity Credentials: Certificates* [Ref 15]. The validated claims and the validated identity of the entity signing the claims can be used to determine the level of trust in the originating entity and their asserted SIP RPH information.

5.1.2 RFC 8224: Authenticated Identity Management in the Session Initiation Protocol (SIP)

IETF RFC 8224 [Ref 13] defines a SIP-based framework for an authentication service and verification service for using the PASSporT signature in a SIP INVITE. It defines a new Identity header field that delivers the PASSporT signature and other associated parameters. The authentication service adds the Identity header field and signature to the SIP INVITE generated by the originating provider.[4] The SIP INVITE is delivered to the destination provider, which uses the verification service, to verify the signature using the identity in the P-Asserted-Identity header field or From header field.

[4] Note that when using the Ms reference point defined in 3GPP TS 24.229 [Ref 2] to interact with the authentication service, the authentication service will return identityHeader parameter(s) in the signingResponse(s) and the element that sends the signingRequest (i.e., the IBCF) will be responsible for populating the Identity headers in the outgoing SIP INVITE message.

5.1.3 RFC 8443: Personal Assertion Token (PASSporT) Extension for Resource Priority Authorization

IETF RFC 8443 [Ref 16] defines an optional extension to the PASSporT and the associated STI mechanisms to support the signing of the SIP Resource-Priority Header field. It extends the PASSporT to allow cryptographic signing of the SIP Resource-Priority Header field which is used for communications resource prioritization. It also describes how the PASSPorT extension is used in SIP signaling to convey assertions of authorization of the information in the SIP Resource-Priority Header field.

Specifically, assertion of the information in the RPH includes a "ppt" extension with an "rph" claim in the PASSporT. Based on IETF RFC 8443 [Ref 16], a PASSporT header with the "ppt" extension will consist of the following information:

```
{

"typ":"passport",

"ppt":"rph",

"alg":"ES256",

"x5u":"https://www.example.org/cert.cer"

}
```

According to IETF RFC 8443 [Ref 16], the "rph" claim will provide an assertion of authorization for the information in the SIP RPH. In the context of emergency calls and callback calls, the "rph" claim will provide an assertion of the value of the SIP RPH. Specifically, the "rph" claim includes an assertion of the priority level to be used for a given communication session.

5.1.4 Assertion Values

RFC 9027 [Ref 7] adds new assertion values for the Resource-Priority Header ("rph") claim defined in IETF RFC 8443 [Ref 16] to support Emergency Services Networks for emergency call origination and callback.

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

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

In addition, RFC 9027 [Ref 7] defines a new SIP Priority header claim ("sph") for protection of the "psap-callback" value as part of the "rph" PASSporT extension to support the security of Emergency Services Networks for emergency callbacks. The "sph" claim shall only be used for authorized emergency callbacks and corresponds to a SIP Priority header field with the value "psap-callback". For emergency callbacks, the "orig" claim of the "rph" PASSporT represents the PSAP telephone number. The "dest" claim contains the telephone number representing the emergency caller that is being called back. The following is an example of an "rph" claim for a SIP Resource-Priority Header field with an "esnet.0" assertion and an "sph" claim:

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

```
}
```

After the PASSporT header and claims have been constructed, their signature shall be generated normally per the guidance in IETF RFC 8225 [Ref 14] using the full form of PASSporT.

5.2 Governance Model and Certificate Management

The credentials (i.e., the STI certificate) used to create the signature shall have authority over the namespace of the "rph" claim and the content of the "sph" claim. There is only one authority per claim. The authority shall use its credentials associated with the specific service supported by the resource priority namespace in the claim.

The governance model and the management of the credentials used by Originating Service Providers (for emergency originations) and NG9-1-1 System Service Providers (for callback calls) for cryptographic signing of the SIP RPH and Priority header are not within the scope of this standard.

5.3 Reference Architecture

5.3.1 Emergency (9-1-1) Originations

Figure 5-1 shows a reference architecture for SIP RPH signing in the context of emergency originations. The architecture used for signing the SIP RPH associated with emergency originations builds on the calling number authentication/verification architecture supported by 3GPP TS 24.229 [Ref 2] and 3GPP TS 23.228 [Ref 1] in which an IBCF in an originating network, if configured through operator policies, invokes an Application Server via the Ms reference point for the signing of identity information, if available, in an incoming request. The IBCF then includes the signed information in the outgoing request. In Figure 5-1, the emergency call is originated from Originating Service Provider A's network that performs the authentication service and is terminated in NG9-1-1 Emergency Services Network Provider 1's network, which performs the verification service.

As described in Clause V.2.1 of 3GPP TS 24.229 [Ref 2], the Ms reference point is used to request the signing of an Identity header field or to request verification of a signed identity in an Identity header field. The currently defined protocol to be used on the Ms Reference Point is HTTP 1.1, as specified in IETF RFC 7230 [Ref 12].

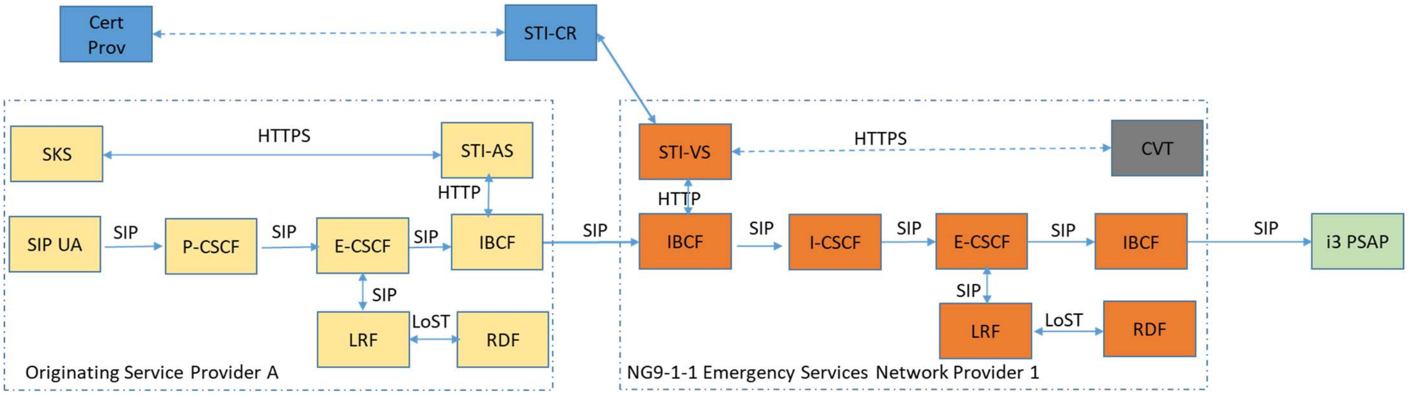

Figure 5-1: Architecture for Signing SIP RPH of Emergency Originations

The reference architecture illustrated in Figure 5-1 includes the following elements:

IMS Elements:

- SIP User Agent (SIP UA) – This component represents the originating end point for an emergency origination.

- Proxy Call Session Control Function (P-CSCF) – This component receives the emergency session establishment request from the UA, detects that it is an emergency session request, and forwards it to/towards the E-CSCF.

  NOTE: As specified in 3GPP TS 24.229 [Ref 2] and ATIS-0700015.v004, *ATIS Standard for Implementation of 3GPP Common IMS Emergency Procedures for IMS Origination and ESInet/Legacy Selective Router Termination*, if required by operator policy, the P-CSCF may forward the emergency session establishment request to the E-CSCF via an S-CSCF.

- Emergency Call Session Control Function (E-CSCF) – In the context of an originating IMS network, the E-CSCF receives the emergency session establishment request from the P-CSCF, obtains location information, obtains routing information, and forwards the emergency session establishment request per the routing information. In the context of an NG9-1-1 Emergency Services Network, the E-CSCF receives the emergency session establishment request from the I-CSCF, queries the LRF for routing information, and then forwards the call request towards the appropriate PSAP per the routing information. After initial call routing to the appropriate PSAP, the E-CSCF may or may not remain in the call path per implementation.
- Location Retrieval Function (LRF) - The LRF obtains location information for a UA and uses that location to acquire routing information for an emergency session from the Routing Determination Function (RDF).
- Routing Determination Function (RDF) - This functional entity, which may be integrated in a Location Server or in an LRF, provides routing information for an emergency session to the E-CSCF.
- Interconnection Border Control Function (IBCF) – This function is at the edge of the service provider network and represents the Network-to-Network Interface (NNI) or peering interconnection point between telephone service providers. It is the entry and exit point for SIP calls between providers.
- Interrogating Call Session Control Function (I-CSCF) – This component receives emergency call requests from the entry IBCF in an NG9-1-1 Emergency Services Network. The I-CSCF forwards the emergency call request to the provisioned (or pre-configured) E-CSCF in the NG9-1-1 Emergency Services Network.

SHAKEN Elements

- Secure Telephone Identity Authentication Service (STI-AS) – Defined in ATIS-1000074-E [Ref 5] as an application server that performs the function of the authentication service defined in IETF RFC 8224 [Ref 13]. In the context of this standard, the STI-AS contains a logical component that provides the authentication service for the SIP RPH signing defined in IETF RFC 8443 [Ref 16].
- Secure Telephone Identity Verification Service (STI-VS) – Defined in ATIS-1000074-E [Ref 5] as an application server that performs the function of the verification service defined in IETF RFC 8224 [Ref 13]. In the context of this standard, the STI-VS contains a logical component that provides the verification service for the SIP RPH signing defined in IETF RFC 8443 [Ref 16].
- Call Validation Treatment (CVT) – Defined in ATIS-1000074-E [Ref 5] as a logical function that could be an application server function or a third-party application for applying anti-spoofing mitigation techniques once the caller identity signature, if available, is positively or negatively verified.
- Secure Key Store (SKS) – Defined in ATIS-1000074-E [Ref 5] as a highly secure logical element that stores secret private key(s) for the STI-AS to access. (Any element that accesses the key store (i.e., STI-AS) should also be highly secure.)
- Certificate Provisioning Service – Defined in ATIS-1000074-E [Ref 5] as a logical service used to provision certificate(s) used for STI.
- Secure Telephone Identity Certificate Repository (STI-CR) – Defined in ATIS-1000074-E [Ref 5] as a publicly accessible store for public key certificates.

Public Safety Elements

- i3 Public Safety Answering Point (PSAP) – A PSAP is an entity responsible for receiving emergency (9-1-1) calls and processing those calls according to a specific operational policy. An i3 PSAP is a SIP end point (client) that is capable of receiving IP-based signaling and media associated with emergency calls in a manner conformant with NENA i3 standards.

5.3.2 Callback Calls

Figure 5-2 shows a reference architecture for SIP RPH and Priority header signing in the context of callback calls. The architecture used for signing the SIP RPH and Priority header associated with callback calls assumes that a Transit Function in an IMS NG9-1-1 Emergency Services Network, if configured through operator policies, invokes caller identity authentication and RPH/SIP Priority header signing by passing the SIP INVITE message associated with the callback call via the Mf reference point to the STI-AS. Specifically, a Transit Function processing a SIP INVITE associated with a callback call will interact with the STI-AS to assert the telephone identity of the caller (i.e., a P-Asserted-Identity header field containing sip:TN@<psapdomain>;user=phone, where the TN is associated with the PSAP originating the callback call) and to request signing of the RPH value (i.e., "esnet.0") and the SIP Priority header value (i.e., "psap-callback") included in the SIP INVITE message associated with the callback call. The Transit Function will invoke the STI-AS for callback calls presented to it after call processing has completed, that is, after the target interconnected network has been determined.

Once the assertion and signing process is completed, the Transit Function will receive the SIP INVITE back from the STI-AS with two added SIP Identity header fields constructed per IETF RFC 8224 [Ref 13], one associated with the caller identity and one associated with the RPH/SIP Priority header, using the IMS-based NG9-1-1 Emergency Services Network provider’s credentials as the signing authority for the PSAP telephone identity and RPH/SIP Priority header.

After receiving the SIP INVITE from the STI-AS, the Transit Function will route the call to the exit IBCF. The exit IBCF will then route the call over the NNI through the standard inter-domain routing configuration towards the entry IBCF associated with the emergency caller’s home network. The home network will perform STI verification, assuming it supports such capabilities, and presents the called party (i.e., the emergency caller) with an indication of the verification status of the caller identity and RPH/SIP Priority header.

Note that an alternative callback architecture will have the exit IBCF in the NG9-1-1 Emergency Services Network interact with the STI-AS via the Ms reference point, using the HTTP interface described in Annex V of 3GPP TS 24.229 [Ref 2], rather than having the transit function interact with the STI-AS using SIP. See ATIS-0500032 [Ref 3] for further details. An alternative callback architecture will allow the CSCF in the emergency caller’s home network to interact with the STI-VS using SIP, rather than having the IBCF interact with the STI-VS using HTTP (as illustrated below).

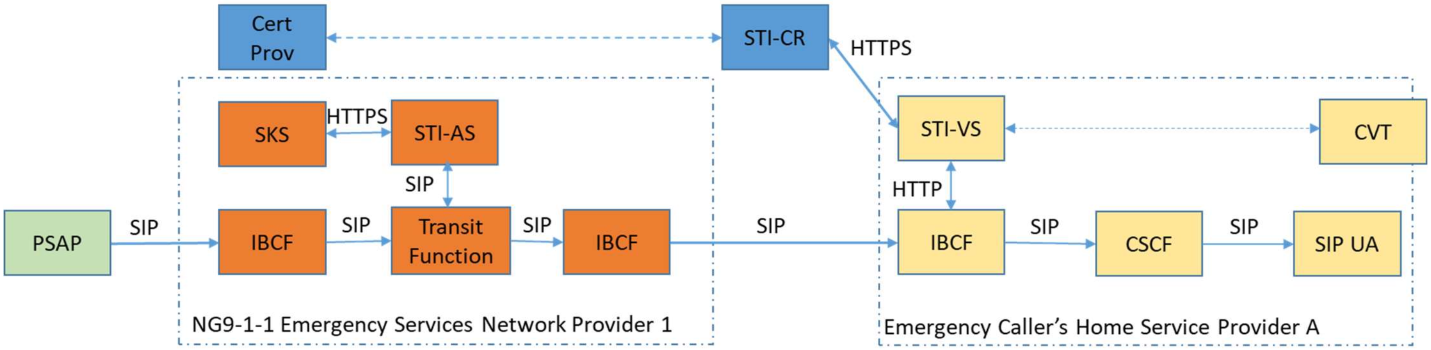

Figure 5-2: Architecture for Signing SIP RPH of Callback Calls

In addition to the elements described in Clause 5.3.1, the reference architecture illustrated in Figure 5-2 includes the following IMS element:

- Transit Function – As described in 3GPP TS 23.228 [Ref 1], a Transit Function is an element that determines where to route a session based on an analysis of the destination address. This includes routing to destinations in other IMS networks or the PSTN. In the context of the emergency calling, the Transit Function will be used to support multimedia callbacks.

5.4 Call Flows

5.4.1 Emergency (9-1-1) Originations

This call flow description is based on the reference architecture illustrated in Figure 5-1.

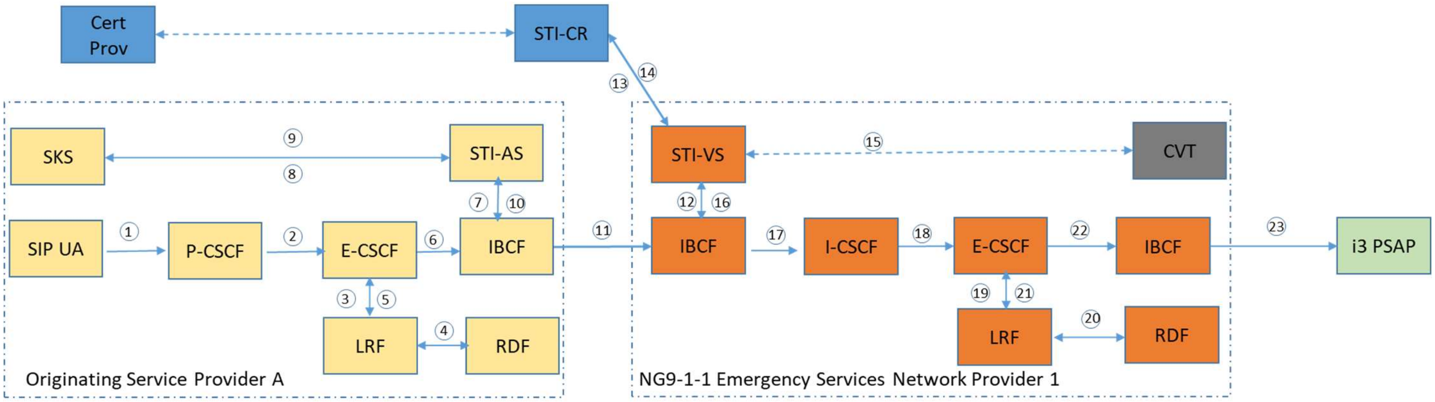

Figure 5-3: Emergency Origination SIP RPH Signing Call Flow

1. The originating SIP UA, which first registers and is authenticated to the P-CSCF, creates a SIP INVITE with a telephone number identity.
2. The P-CSCF in the originating network adds a P-Asserted-Identity header field asserting the caller identity of the originating SIP UA, and an RPH with value "esnet.1". If supported by local policy, the P-CSCF will also insert a "verstat" parameter in the P-Asserted-Identity header, and optional Attestation-Info and Origination-Id header fields. The P-CSCF forwards the SIP INVITE to the E-CSCF.
3. The E-CSCF sends the SIP INVITE to the LRF to determine routing instructions.
4. The LRF acquires location, if required, and queries the RDF for the routing URI.
5. The LRF returns the routing URI to the E-CSCF.
6. If the emergency call is to be routed to an NG9-1-1 Emergency Services Network, the E-CSCF forwards the emergency call to the exit IBCF.
7. The exit IBCF sends an HTTP POST message containing two signing requests over the Ms reference point to the STI-AS.
   a. The signingRequest associated with the caller identity includes an "attest" parameter that contains the attestation information and an "origid" parameter, as well as other PASSporT information (i.e., "orig", "dest", and "iat"). The "attest" parameter and the "origid" parameter are either populated according to local policy, or based on information received by the IBCF in the Attestation-Info header and Origination-Id header within the SIP INVITE.
   b. The signingRequest associated with the RPH includes an "rph" claim that contains an "auth" key that asserts the value "esnet.1", along with the "orig", "dest", and "iat". The IBCF will populate the assertion value in the signingRequest based on the RPH field value received in incoming signaling.

   NOTE: The STI-AS must be invoked after originating call processing (e.g., after routing URI has been determined).

8. The STI-AS in the Originating Service Provider (i.e., Service Provider A) network determines through service provider-specific means the legitimacy of the content of the caller identity and the RPH field (i.e., the value in the "esnet" namespace) sent to it in the HTTP signingRequest. The STI-AS then securely requests its private key from the SKS.
9. The SKS provides the private key in the response, and the STI-AS signs and populates an identityHeader parameter as a JSON object in each signingResponse per 3GPP TS 24.229 [Ref 2].

10. The STI-AS returns an HTTP 200 OK message that includes a signingResponse that contains the signed identityHeader field value for the caller identity and a signingResponse that contains the signed identityHeader field value for the RPH.
11. The exit IBCF uses the identityHeader parameters in the two signing responses to populate Identity headers in the SIP INVITE message, then routes the SIP INVITE (with the Identity headers) over the NNI using standard inter-domain routing resolution. The IBCF will remove the "verstat" parameter from the P-Asserted-Identity header prior to sending the call to the Emergency Services Network.

    NOTE: As an implementation option, the Originating Service Provider may determine, based on the capabilities of the target Emergency Services Network, what information related to caller identity and RPH authentication will be forwarded to the interconnected network.

12. Upon receiving the SIP INVITE, the entry IBCF in the NG9-1-1 Emergency Services Network sends an HTTP POST containing a verificationRequest to the STI-VS. The verificationRequest includes an identityHeader parameter corresponding to the Identity header containing the signed caller identity information, an identityHeaders parameter corresponding to the Identity header containing the signed RPH information, as well as the "to" parameter containing the destination identity from the To header, the "from" parameter containing the asserted identity from the From or P-Asserted-Identity, and a "time" parameter based on the Date header field in the incoming SIP INVITE.

    NOTE: The STI-VS must be invoked before terminating call processing (e.g., before routing URI has been determined).

13. The NG9-1-1 Emergency Services Network provider STI-VS determines the STI-CR Uniform Resource Identifier (URI) and makes an HTTPS request to the STI-CR as per ATIS-1000074-E [Ref 5].
14. The STI-VS validates the certificate and then extracts the public key as per ATIS-1000074-E [Ref 5]. It constructs the IETF RFC 8224 [Ref 13] format and uses the public key to verify the signature in the identityHeader and identityHeaders parameters, which validates the caller identity and RPH field signed by the originating service provider STI-AS.
15. The STI-VS may interact with the CVT based on local policy and agreements between the 9-1-1 Authority and the analytics/CVT provider.
16. The STI-VS returns a verificationResponse to the entry IBCF. The verificationResponse includes a "verstatValue" parameter that contains the results of the verification process associated with the signed caller identity and a "verstatPriority" parameter that contains the results of the verification process associated with the signed RPH. Depending on the results of the verification process, the "verstatValue" associated with the signed caller identity shall be set to "TN-Validation-Passed", "TN-Validation-Failed", or "No-TN-Validation", and the "verstatPriority" associated with the signed RPH shall be set to "RPH-Validation-Passed", "RPH-Validation-Failed", or "No-RPH-Validation".
17. The entry IBCF populates the content of the "verstatValue" in a "verstat" parameter within the P-Asserted-Identity header and the content of the "verstatPriority" in the Priority-Verstat header field in the SIP INVITE, and passes the SIP INVITE to the I-CSCF in the NG9-1-1 Emergency Services Network.
18. The I-CSCF passes the SIP INVITE to the pre-configured E-CSCF.
19. The E-CSCF forwards the SIP INVITE to the LRF.
20. The LRF queries the RDF using the location information received in the SIP INVITE message and the emergency service Uniform Resource Name (urn:service:sos). The RDF returns a routing URI. In this example, the routing URI is associated with an i3 PSAP that is served by the NG9-1-1 Emergency Services Network.
21. The LRF redirects the call back to the E-CSCF, passing the Routing (PSAP) URI.
22. 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.

23. The (exit) IBCF forwards the SIP INVITE to the i3 PSAP with the appropriate "verstat" value in the P-Asserted-Identity header, the Priority-Verstat header field and the Identity headers, and normal call processing associated with the emergency origination continues.[5]

5.4.2 Callback Calls

This call flow description is based on the reference architecture illustrated in Figure 5-2.

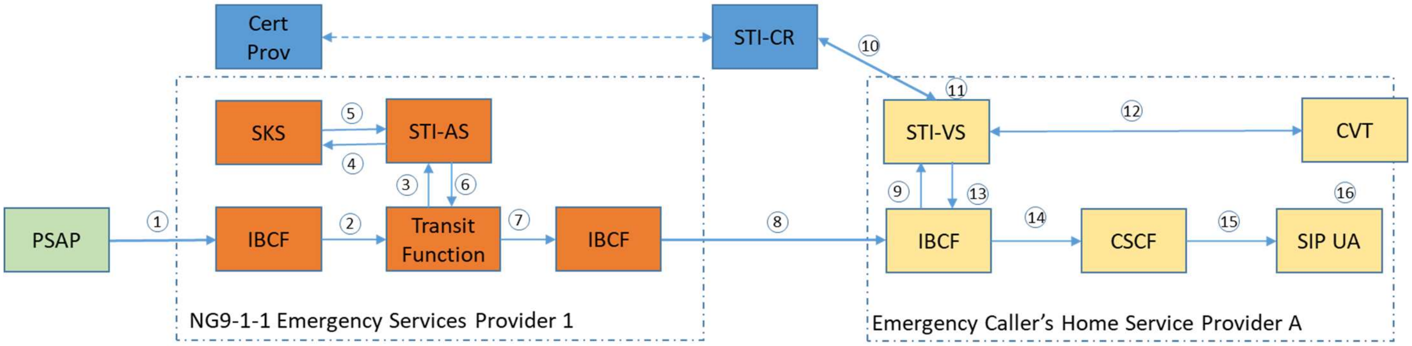

Figure 5-4: Callback Call SIP RPH Signing Call Flow

1. The PSAP Call Handling Function initiates a callback call with the callback URI from the original emergency call in the To header and Request-URI, the TN of the PSAP originating the callback (i.e., sip:TN@<psapdomain>;user=phone) in the From and P-Asserted-Identity headers, "psap-callback" in the Priority header, and "esnet.0" in the Resource-Priority Header.
2. Upon receiving the SIP INVITE from the PSAP, the entry IBCF applies general screening rules to the request and, based on local policy, adds an Origination-Id header, to indicate from where the request was received, and an Attestation-Info header to the SIP INVITE. It then forwards the SIP INVITE to the Transit Function.
3. The Transit Function uses the destination address (i.e., the callback URI) in the Request-URI to determine the routing for the call. Before forwarding the call to the interconnecting network, the Transit Function sends the request to the STI-AS for authentication and signing of the caller identity and signing of the RPH and Priority header.

   NOTE: The STI-AS must be invoked after originating call processing (i.e., after the Transit Function determines that the interconnected network over which the call will be routed is an IP network).

4. The STI-AS determines, through service provider-specific means, the legitimacy of the content of the caller identity and the RPH and SIP Priority header fields. The STI-AS then securely requests its private key from the SKS.
5. The SKS provides the private key in the response, and the STI-AS signs and adds Identity header fields per IETF RFC 8224 [Ref 13].
6. The STI-AS returns the SIP INVITE which includes a signed Identity header field value for the caller identity and signed Identity header field values for the RPH and SIP Priority header in JSON objects.
7. The Transit Function routes the SIP INVITE (with the Identity headers) to the exit IBCF using standard inter-domain routing resolution. If, based on local policy, a "verstat" parameter is present in the SIP INVITE received by the Transit Function, the IBCF shall remove it before forwarding the call to the next network.

[5] Delivery of the Identity headers allows PSAP call takers to use attestation level and verification status information to influence the handling of emergency calls.

8. In this example, the exit IBCF forwards the SIP INVITE to the entry IBCF in the emergency caller's home network. Note that, depending on the scenario, the callback call may traverse other interconnecting networks.
9. The emergency caller's home service provider's (Service Provider A) entry IBCF initiates a verificationRequest to the STI-VS that includes an identityHeader parameter associated with the caller identity and an identityHeaders parameter associated with the RPH/SIP Priority header.

   NOTE: The STI-VS must be invoked before terminating call processing (e.g., before routing URI has been determined).

10. The emergency caller's home service provider STI-VS uses the "x5u" field in the PASSporT Protected Header per IETF RFC 8225 [Ref 14] to determine the STI-CR Uniform Resource Identifier (URI) and makes an HTTPS request to the STI-CR.
11. The STI-VS validates the certificate and then extracts the public key as per ATIS-1000074-E [Ref 5]. It constructs the IETF RFC 8224 [Ref 13] format and uses the public key to verify the signature in the Identity header fields, which validates the caller identity and the RPH and SIP Priority header field content used when the caller identity and RPH/SIP Priority header content were signed by the STI-AS.
12. The STI-VS may interact with the CVT based on local policy and agreements between the emergency caller's home service provider and the analytics/CVT provider.
13. Depending on the result of verification, the STI-VS includes an appropriate indicator of the verification result and returns a verificationResponse containing a verstatValue parameter (associated with the "identityHeader" parameter in the verificationRequest) and a "verstatPriority" parameter (associated with the "rph" claim in the "identityHeaders" parameter in the verificationRequest) to the IBCF. The "verstatValue" associated with the signed caller identity shall be set to "TN-Validation-Passed", "TN-Validation-Failed", or "No-TN-Validation", and the "verstatPriority" associated with the signed RPH/SIP Priority header shall be set to "ECB-RPH-Validation-Passed", "ECB-RPH-Validation-Failed", or "No-ECB-RPH-Validation".
14. The IBCF populates the content of the "verstatValue" in a "verstat" parameter within the P-Asserted-Identity header and the content of the "verstatPriority" in the Priority-Verstat header field in the SIP INVITE, and continues to set up the callback call to the CSCF. If a value of "ECB-RPH-Validation-Failed" is populated in the Priority-Verstat header field, the processing of the RPH and Priority header fields by the emergency caller's home network will be based on local policy; e.g., the network could choose to ignore these header fields.
15. The CSCF continues to set up the callback call towards the emergency caller.
16. The terminating SIP UA receives the SIP INVITE and normal SIP processing of the call continues, returning "200 OK" or optionally setting up media end-to-end.

6 Procedures for SIP RPH and Priority Header Authentication

This normative clause will detail the procedures at key elements in the architecture that play a role in asserting, signing and verifying the information in the SIP RPH and Priority header fields in the context of emergency calling.

6.1 Procedures at the IBCF

The IBCF shall adhere to Clauses 4 and 5.10 in 3GPP TS 24.229 [Ref 2] with additions as noted below. For emergency originations, an IBCF will be the exit point from the Originating Service Provider network and the entry point to an IMS NG9-1-1 Emergency Services Network. For emergency originations, there will also be an exit IBCF between the NG9-1-1 Emergency Services Network and the PSAP. For callback calls, there will be an IBCF at the entry point of the IMS NG9-1-1 Emergency Services Network facing the PSAP and an IBCF that will be the exit point from the NG9-1-1 Emergency Services Network to the interconnected network. There will also be an IBCF at the entry point into an interconnected network.

6.1.1 Entry IBCF

For emergency (9-1-1) originations, the entry IBCF associated with the NG9-1-1 Emergency Services Network will perform normal border control functions. As described in Clause 5.10.10.2 of 3GPP TS 24.229 [Ref 2], when receiving an initial SIP INVITE containing one or more SIP Identity header fields, the IBCF shall determine the caller identity to be verified by decoding the Identity header field containing a PASSporT SHAKEN JSON Web Token. The IBCF shall also determine the RPH value to be verified by decoding the Identity header associated with the signed RPH. The IBCF shall then build and send a verificationRequest to the STI-VS, assuming the Ms reference point. Upon receiving a verificationResponse with a "verstatValue" parameter reflecting the verification status of the Identity header associated with calling identity, the IBCF shall add this parameter to the verified identity in the SIP From header field or the SIP P-Asserted-Identity header field in the forwarded SIP request. If a "verstat" parameter is already present in the From or P-Asserted-Identity header of the received SIP INVITE, the entry IBCF shall remove it. The entry IBCF shall also populate a Priority-Verstat header field in the outgoing SIP INVITE, based on the associated "verstatPriority" parameter returned in the verificationResponse, to convey the verification status of the Identity header associated with the RPH.

As the first active SIP element in an NG9-1-1 Emergency Services Network in the path of an emergency call, the entry IBCF shall add the Call Identifier, Incident Tracking Identifier, and a Resource-Priority Header set to "esnet.1" (if not already present) to the SIP INVITE associated with the emergency call. The entry IBCF will ensure that the Resource-Priority Header is set to "esnet.1" to indicate an emergency call. See ATIS-0500032 [Ref 3] for further details. The entry IBCF forwards the SIP INVITE to the I-CSCF.

For callback calls, the entry IBCF in the NG9-1-1 Emergency Service Network (i.e., the IBCF facing the PSAP) will perform normal border control functions, and once the message is validated, it will forward the SIP INVITE to the Transit Function. If the SIP INVITE received by the entry IBCF contains a "verstat" parameter in the From or P-Asserted-Identity header, the entry IBCF shall remove it. As the first active SIP element in an NG9-1-1 Emergency Services Network in the path of a callback call, the IBCF shall add a Resource-Priority Header set to "esnet.0" (if not already present) to the SIP INVITE associated with the callback call. Based on local policy, the entry IBCF may also add an Origination-Id header, indicating from where the request was received, and an Attestation-Info header to the SIP INVITE.

For callback calls, the entry IBCF in the interconnected network (i.e., the Service Provider network interconnected to the NG9-1-1 Emergency Services Network via the IP NNI) will perform normal border control functions, and once the message is validated, it will forward the SIP INVITE based on normal routing procedures.

Also for callback calls, based on local policy, the entry IBCF in the emergency caller’s home network may build and send a verificationRequest to the STI-VS, via the Ms reference point. Upon receiving a verificationResponse with a "verstatValue" parameter reflecting the verification status of the Identity header associated with calling identity, the IBCF shall add a "verstat" parameter reflecting the content of the "verstatValue" parameter to the verified identity in the SIP From header field or the SIP P-Asserted-Identity header field in the forwarded SIP request. The entry IBCF shall also populate the verification status associated with the signed RPH/SIP Priority header in a Priority-Verstat header field in the forwarded SIP request, based on the associated "verstatPriority" parameter returned in the verificationResponse.

6.1.2 Exit IBCF

For an emergency (9-1-1) origination, the exit IBCF in the Originating Service Provider network can interact with an STI-AS via the Ms reference point for the signing of caller identity and RPH information, if available in an incoming request. Specifically, the exit IBCF sends an HTTP POST containing two signing requests over the Ms reference point to the STI-AS. The signingRequest associated with the caller identity will include an "attest" parameter that contains the attestation information and an "origid" populated based on local policy or received by the IBCF in Attestation-Info and Origination-Id headers, respectively, as well as other PASSporT information (i.e., "orig", "dest", and "iat"). The signingRequest associated with the RPH shall include an "rph" claim as described in IETF RFC 8443 [Ref 16] that contains an "auth" key and assertion value of "esnet.1", as described in RFC 9027 [Ref 7], along with the "orig", "dest", and "iat". The exit IBCF shall populate the assertion value in the signingRequest based on the RPH field in the received SIP INVITE. The exit IBCF includes the signed Identity headers received in the HTTP signing responses in the outgoing request. The exit IBCF shall remove the "verstat" parameter, if any, from the From header or P-Asserted-Identity header prior to sending the SIP INVITE over the IP NNI to the Emergency Services Network. As described in Clause 5.4.1, the Originating Service Provider may, as an implementation option, determine what other information related to caller identity and RPH authentication will be forwarded to the interconnected network, based on the capabilities of the target Emergency Services Network.

For an emergency (9-1-1) origination, the exit IBCF in the NG9-1-1 Emergency Services Network shall use the Route header to determine where to forward the SIP INVITE (e.g., to the i3 PSAP). The IBCF shall pass all headers and message bodies unless passing of the parameters is prohibited by its role as a border gateway function.

For callback calls, if the NG9-1-1 Emergency Services Network supports caller identity authentication and RPH and SIP Priority header signing, the exit IBCF may, based on local policy, be responsible for interacting with an STI-AS. If so, the exit IBCF will send an HTTP POST containing two signing requests, assuming the Ms reference point to the STI-AS. The signingRequest associated with the caller identity will include an "attest" parameter that contains the attestation information and an "origid" populated based on local policy or received by the IBCF in Attestation-Info and Origination-Id headers, respectively, as well as other PASSporT information (i.e., "orig", "dest", and "iat"). The signingRequest associated with the RPH/Priority header will include an "rph" claim that contains an "auth" key and assertion value of "esnet.0" and a "sph" claim set to "psap-callback", as described in RFC 9027 [Ref 7], along with an "orig", "dest", and "iat". The exit IBCF shall use the identityHeader parameters received in the signing responses from the STI-AS to populate Identity headers in the outgoing SIP INVITE associated with the callback call.

In support of callback calls, the exit IBCF in the NG9-1-1 Emergency Services Network shall use the Route header to determine the well-known URI associated with the interconnected network. The IBCF shall pass all headers and message bodies unless passing of the parameters is prohibited by its role as a border gateway function.

6.2 Procedures at the STI-AS

In the context of emergency (9-1-1) originations, the STI-AS, assuming the Ms reference point, will receive an HTTP POST from the IBCF that includes a signingRequest that contains a SHAKEN PASSporT (i.e., "attest", "dest", "iat", "orig", "origid"), as well as a signing request that contains an "rph" claim. The STI-AS determines through service provider-specific means the legitimacy of the content of the caller identity and the "rph" claim (i.e., the value in the "esnet" namespace), then securely requests its private key from the SKS. Upon receiving the private key from the SKS, the STI-AS signs and returns to the IBCF an identityHeader field value for the caller identity and an identityHeader field value for the RPH in JSON objects in signing responses within an HTTP 200 OK.

In the context of callback calls, the STI-AS may, based on local policy, receive SIP INVITE messages associated with callback calls from a Transit Function and will be responsible for determining, through service provider-specific means, the legitimacy of the caller identity, RPH, and SIP Priority header being used in the SIP INVITE. The STI-AS is then responsible for cryptographically signing the PASSporT and adding Identity header fields with signatures (corresponding to the caller identity and RPH/SIP Priority header) to the SIP INVITE that it returns to the Transit Function. Alternatively, an STI-AS may, based on local policy and assuming the Ms reference point, receive an HTTP POST from an exit IBCF that includes a signingRequest containing SHAKEN PASSporT claims (i.e., "attest", "dest", "iat", "orig", "origid"), as well as a signing request that contains an "rph" claim and an "sph" claim. The STI-AS determines through service provider-specific means the legitimacy of the content of the caller identity and the "rph" and "sph" claims and securely requests its private key from the SKS. The STI-AS then signs and returns to the IBCF an identityHeader parameter for the caller identity and an identityHeader parameter for the RPH/Priority header as JSON objects in signing responses within an HTTP 200 OK.

6.3 Procedures at the STI-VS

The STI-VS is an application server that performs the function of the verification service defined in IETF RFC 8224 [Ref 13]. In the context of emergency calling, the STI-VS provides verification services applicable to emergency calls destined for PSAPs that are served by an NG9-1-1 Emergency Services Network and callback calls destined for the emergency caller. Associated with an emergency (9-1-1) origination, the STI-VS will receive an HTTP verificationRequest from an entry IBCF in the IMS NG9-1-1 Emergency Services Network via the Ms reference point. Associated with a callback call, the STI-VS will receive a verificationRequest in one of two ways: by receiving an HTTP verificationRequest over an Ms reference point from an IBCF in the emergency caller's home network, or by receiving a SIP INVITE from a CSCF in the emergency caller's home network. The STI-VS retrieves the certificate referenced by the "x5u" field in the PASSporT protected header from the STI-CR, and follows the basic certificate path processing as described in IETF RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, following the chain until the root is reached. The STI-VS ensures that the root certificate is on the list of trusted Secure Telephone Identity Certification Authorities (STI-CAs). The STI-VS validates that the PASSporT information provided in the Identity headers contained in the verificationRequest includes the SHAKEN claims and "rph" claim. The verifier shall also follow the verification procedures defined in

IETF RFC 8224 [Ref 13] to check the corresponding date, origination and destination identities, with the restrictions specified in ATIS-1000074-E [Ref 5]. If an Ms reference point is used to interact with the ST-VS, the STI-VS will return a "verstatValue" parameter (associated with the "identityHeader" parameter in the verificationRequest) and a "verstatPriority" parameter (associated with the "rph" claim in the "identityHeaders" parameter in the verificationRequest) in an HTTP verificationResponse. If a SIP interface is used to interact with the STI-VS, the STI-VS will return a "verstat" parameter in the P-Asserted-Identity or From header, and a Priority-Verstat header field in a SIP INVITE to convey the results of the verification. (See Clauses 5.4.1 and 5.4.2 for further details.) The STI-VS may include another appropriate indicator (not defined in this document) in the verificationResponse based on interactions with the CVT. The STI-VS must be invoked prior to terminating call processing associated with the emergency call (e.g., before routing URI is determined).

6.4 Procedures at the P-CSCF

A P-CSCF operating in an Originating Service Provider network that supports caller identity authentication and RPH signing may, based on local policy, be responsible for inserting attestation information related to the asserted caller identity and populating the RPH in a SIP INVITE associated with an emergency origination. According to 3GPP TS 24.229 [Ref 2], when a node performs attestation of an identity in an incoming request or can attest to the origin of the request, the node can inform a downstream node about what kind of attestation the node has performed. Based on local policy, if the P-CSCF is responsible for providing attestation information associated with the caller identity for an authenticated emergency call, the P-CSCF will insert a "verstat" parameter in the P-Asserted-Identity header, an optional Attestation-Info header field in the SIP INVITE with a value of "A", "B" or "C", as defined in ATIS-1000074-E [Ref 5], associated with the caller identity, and an optional origination identifier in an Origination-Id header field. The P-CSCF may also populate a value of "esnet.1" in the RPH.

6.5 Procedures at the Transit Function

The Transit Function is expected to adhere to the procedures described in Clauses 4.15.3 and 5.19 of 3GPP TS 23.228 [Ref 1] with the following clarifications.

When a PSAP initiates a callback call via an IMS NG9-1-1 Emergency Services Network, the Transit Function will be responsible for routing the callback call based on the destination address (i.e., the address associated with the emergency caller) received in incoming signaling. A Transit Function operating in an NG9-1-1 Emergency Services Network that supports caller identity authentication and RPH and SIP Priority header signing may, based on local policy, be responsible for interacting with an STI-AS to assert the telephone identity of the caller (i.e., the PSAP) and to request the signing of the RPH and SIP Priority header values prior to forwarding the callback request towards the succeeding network via an exit IBCF. The Transit Function will utilize a SIP interface to the STI-AS, passing along the SIP INVITE message that it received from the entry IBCF. The Transit Function will invoke the STI-AS for callback calls after call processing has completed, that is, after the Transit Function determines the interconnected network to which the call will be routed. Once the assertion and signing process is completed, the Transit Function will receive the SIP INVITE back from the STI-AS with an added SIP Identity header field (associated with the caller identity) constructed per IETF RFC 8224 [Ref 13], using the IMS-based NG9-1-1 Emergency Services Network provider’s credentials as the signing authority for the PSAP telephone identity. The SIP INVITE returned by the STI-AS will also include an Identity header associated with the RPH/SIP Priority header. After receiving the SIP INVITE from the STI-AS, the Transit Function will route the call to the exit IBCF.