**ATIS-10000XX**

ATIS Standard on

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

**Alliance for Telecommunications Industry Solutions**

Approved Month DD, YYYY

**Abstract**

This standard defines how the IETF Personal Assertion Token (PASSporT) Extension for Resource-Priority Authorization (IETF RFC 8443) with the extensions defined in draft-ietf-stir-rph-emergency-services-01 and the associated STIR mechanisms are used to sign the Session Initiation Protocol (SIP) Resource-Priority Header (RPH) header field and convey assertions of Resource-Priority associated with an emergency call or callback call. Specifically, this standard describes a procedure for providing cryptographic authentication and verification of the information in the SIP RPH 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 [**COMMITTEE NAME**] Committee [**INSERT MISSION**]. [**INSERT SCOPE**].

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.

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

At the time of consensus on this document, [**COMMITTEE NAME**], which was responsible for its development, had the following leadership:

[**LEADERSHIP LIST**]

The **[SUBCOMMITTEE NAME]** Subcommittee was responsible for the development of this document.

**Revision History**

| **Date** | **Version** | **Description** | **Author** |
| --- | --- | --- | --- |
| 12/10/2019 | 0.0 | Initial Draft | T. Reese |
| 01/10/2020 | 0.1 | IPNNI-2020-00002R000 | T. Reese |
| 03/02/2020 | 0.2 | IPNNI-2020-00040R000 | T. Reese |
| 05/07/2020 | 0.3 | IPNNI-2020-00069R001 | T. Reese |
| 06/29/2020 | 0.4 | IPNNI-2020-00089R000 | T. Reese |
| 07/13/2020 | 0.5 | IPNNI-2020-00113R000 | T. Reese |

# Table of Contents

[**ATIS-10000XX** i](#_Toc34031447)

[ATIS Standard on i](#_Toc34031448)

[**Session Initiation Protocol (SIP) Resource-Priority Header (RPH) Signing in Support of Emergency Calling** i](#_Toc34031449)

[**Alliance for Telecommunications Industry Solutions** i](#_Toc34031450)

[**Abstract** i](#_Toc34031451)

[Table of Contents iii](#_Toc34031452)

[Table of Figures iv](#_Toc34031453)

[1 Scope & Purpose 1](#_Toc34031454)

[1.1 Scope 1](#_Toc34031455)

[1.2 Purpose 1](#_Toc34031456)

[2 Normative References 2](#_Toc34031457)

[3 Definitions, Acronyms, & Abbreviations 2](#_Toc34031458)

[3.1 Definitions 2](#_Toc34031459)

[3.2 Acronyms & Abbreviations 3](#_Toc34031460)

[4 Assumptions 4](#_Toc34031461)

[4.1 General Assumptions 4](#_Toc34031462)

[4.2 Architectural Assumptions 5](#_Toc34031463)

[5 Overview 6](#_Toc34031464)

[5.1 Protocol Support for SIP RPH Signing of Emergency Calls and Callback Calls 6](#_Toc34031465)

[5.1.1 RFC 8225: PASSporT: Personal Assertion Token 6](#_Toc34031466)

[5.1.2 RFC 8224: Authenticated Identity Management in the Session Initiation Protocol (SIP) 7](#_Toc34031467)

[5.1.3 RFC 8443: Personal Assertion Token (PASSporT) Extension for Resource Priority Authorization 7](#_Toc34031468)

[5.1.4 Assertion Values for a Resource Priority Header Claim in Support of Emergency Services Networks 7](#_Toc34031469)

[5.2 Governance Model and Certificate Management 8](#_Toc34031470)

[5.3 Reference Architecture for SIP RPH Signing 8](#_Toc34031471)

[5.3.1 Reference Architecture for SIP RPH Signing Associated with Emergency (9‑1‑1) Originations 8](#_Toc34031472)

[5.3.2 Reference Architecture for SIP RPH Signing Associated with Callback Calls 9](#_Toc34031473)

[5.4 SIP RPH Signing Call Flows for Emergency Calling 10](#_Toc34031474)

[5.4.1 SIP RPH Signing Call Flow for Emergency Originations 10](#_Toc34031475)

[5.4.2 SIP RPH Signing Call Flow for Callback Calls 12](#_Toc34031476)

[6 Procedures for SIP RPH Signing 13](#_Toc34031477)

[6.1 Procedures at the IBCF 13](#_Toc34031478)

[6.1.1 Entry Point IBCF 14](#_Toc34031479)

[6.1.2 Exit Point IBCF 14](#_Toc34031480)

[6.2 Procedures at the STI-AS 15](#_Toc34031481)

[6.3 Procedures at the STI-VS 15](#_Toc34031482)

[6.4 Procedures at the P-CSCF 15](#_Toc34031483)

[6.5 Procedures at the Transit Function 16](#_Toc34031484)

# Table of Figures

[Figure](#_Toc467601252) 1 Architecture for Signing SIP RPH of Emergency Originations 8

[Figure 2 Architecture for Signing SIP RPH of Callback Calls 10](#_Toc467601253)

[Figure](#_Toc467601252) 3 Emergency Origination SIP RPH Signing Call Flow 11

[Figure 4 Callback Call SIP RPH Signing Call Flow 13](#_Toc467601253)

# Scope & Purpose

## Scope

As specified in [RFC4412], the SIP 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], 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 [RFC 7135]) 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 UE, and when this namespace is used, the trust domain implementation is set to remove it if it occurs from the UE.

Like caller identity information associated with emergency calls and callback calls, the SIP RPH field 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 IP Network-to-Network Interfaces (IP NNIs) from IP originating networks cannot easily determine whether the SIP RPH was populated by an authorized Originating Service Provider or by an unauthorized entity.

This ATIS standard leverages the SHAKEN model specified in [ATIS-1000074] to cryptographically sign and verify the SIP RPH field associated with emergency calls and callback calls using the PASSporT extension defined in [IETF RFC 8443], with the assertion values described in draft-ietf-stir-rph-emergency-services-01, and the associated Secure Telephone Identity (STI) protocols described in [TS 24.229]. Note that application of SIP RPH signing of emergency and callback calls is in addition to the caller identity authentication and verification defined in [ATIS-1000074].

This ATIS standard is intended to provide a framework and guidance on how use the PASSporT extension defined in [IETF RFC 8443], with the assertion values specified in draft-ietf-stir-rph-emergency-services-01 and the associated STI protocols to cryptographically sign and verify the SIP RPH 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 SIP RPH field contents associated with emergency and callback calls (i.e., values in the “esnet” namespace). This standard does not address caller identity authentication and verification associated with emergency calls and callback calls, except in the context of call flow descriptions, nor does it impact specific call processing or routing procedures associated with emergency calls and callback calls. The display of information associated with the verification of SIP RPH values is also outside the scope of this document

## 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. The purpose of this standard is to provide a framework for cryptographically signing the SIP RPH field and verifying that the SIP RPH field can be trusted to mitigate against unauthorized spoofing or tampering of the information conveyed in the SIP RPH. 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], with the assertion values described in draft-ietf-stir-rph-emergency-services-01 can be used for the purpose of providing a trust mechanism for the SIP RPH associated with emergency and callback calls that cross IP NNI boundaries.

# 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.

Editor’s Note: the draft RFCs below will be changed to the normative RFC numbers when available from IETF.

[IETF RFC 4412], *Communications Resource Priority for the Session Initiation Protocol (SIP).*[[1]](#footnote-1)

[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.[[2]](#footnote-2)*

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

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

[IETF RFC 8443], *PASSporT Extension for Resource-Priority Authorization*. 1

[IETF RFC 7135], *Registering a SIP Resource Priority Header Field Namespace for Local Emergency Communications*. 1

[draft-ietf-stir-rph-emergency-services-01], *Assertion Values for a Resource Priority Header Claim in Support of Emergency Services Networks*.1

[IETF RFC 8225], PASSporT: *Personal Assertion Token.*[[3]](#footnote-3)

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

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

[IETF RFC 3325], *Private Extensions to SIP for Asserted Identity within Trusted Networks.*1

[IETF RFC 3261], *SIP: Session Initiation Protocol.*1

[IETF RFC 5280], *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.*1

[IETF RFC 3326], *The Reason Header Field for the Session Initiation Protocol (SIP).*1

[3GPP TS 23.228], *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2.3.2*

[IETF RFC 2616], *Hypertext Transfer Protocol -- HTTP/1.1*.1

[IETF RFC 5280], *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.1

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

[ATIS-0500032.v002], *ATIS Standard for Implementation of an IMS-based NG9-1-1 Service Architecture* (in progress).

# 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> >.

## Definitions

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

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

**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.

## Acronyms & Abbreviations

|  |  |
| --- | --- |
| 3GPP | 3rd Generation Partnership Project |
| AS | Application Server |
| ATIS | Alliance for Telecommunications Industry Solutions |
| B2BUA | Back-to-Back User Agent |
| CRL | Certificate Revocation List |
| CSCF | Call Session Control Function |
| CVT | Call Validation Treatment |
| E-CSCF | Emergency Call Session Control Function |
| 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 |
| JSON | JavaScript Object Notation |
| JWS | JSON Web Signature |
| LRF | Location Retrieval Function |
| NG9-1-1 | Next Generation 9-1-1 |
| NNI | Network-to-Network Interface |
| OCSP | Online Certificate Status Protocol |
| PASSporT | Persona Assertion Token |
| PBX | Private Branch Exchange |
| P-CSCF | Proxy Call Session Control Function |
| PKI | Public Key Infrastructure |
| PSAP | Public Safety Answering Point |
| RDF | Routing Determination Function |
| RFEA | Request for Emergency Assistance |
| SHAKEN | Signature-based Handling of Asserted information using toKENs |
| SIP | Session Initiation Protocol |
| SKS | Secure Key Store |
| SPID | Service Provider Identifier |
| 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 |
| TLS | Transport Layer Security |
| TN | Telephone Number |
| UA | User Agent |
| URI | Uniform Resource Identifier |
| UUID | Universally Unique Identifier |
| VoIP | Voice over Internet Protocol |

# Assumptions

## 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.
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 signing on callback calls.
6. Verification of a signed caller identity/RPH will be performed by the terminating home network for the callback call.
7. A Service Provider can use the same certificates for signing SIP RPH as they use for telephone number (TN) signing, but is not required to do so.
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 is trusted.
9. If validation of the signed caller identity or SIP RPH associated with a 9-1-1 origination fails, the 9-1-1 call will be delivered to the PSAP with caller identity and SIP RPH, as well as the results of the caller identity and RPH verification.

Note: The use of a specific indicator (e.g., ‘verstat’) to convey RPH signing verification success/failure is for further study.

1. If validation of the signed caller identity or SIP RPH associated with a callback call fails, terminating Service Provider local policy will determine terminating call processing, such as whether the call should be delivered with caller identity and/or SIP RPH information intact. Note that if the call proceeds, a verstat parameter will be included in the associated SIP signaling.
2. Signing of caller identity is separate from SIP RPH signing. Separate SIP Identity headers are used for SIP RPH signing and caller identity signing.

## Architectural Assumptions

In keeping with the framework SHAKEN architecture described in [ATIS-1000074], 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 (AS). 3GPP [TS 23.228] and [TS 24.229] do, however, describe the use of the Ms reference point between an IBCF and an AS over which HTTP 1.1, as specified in [RFC 2616], is used. Specifically, Annex V of [TS 24.229] defines a signingRequest/signingResponse and verificationRequest/verificationResponse to support caller identity signing and verification. Note that this mechanism is also supported by [ATIS-1000082], where the egress IBCF in the originating network is the “Authenticator” and the ingress IBCF in the IMS NG9-1-1 Emergency Services Network is the “Verifier”.

Based on [TS 24.229] and [ATIS-1000082], to get an asserted identity signed, the client sends an HTTP POST request towards the signing server containing a PASSporT SHAKEN object. Thus, 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 [TS 24.229], 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 (based on local policy), 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] and [ATIS-1000082], upon receiving an HTTP 200 (OK) response to the signingRequest, the IBCF (Authenticator) will include the value of the "identity" claim in an Identity header field in the forwarded SIP request. This model differs from the framework architecture example described in [ATIS-1000074], 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 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 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 value 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) to the Transit Function, constructed per [RFC 8224]. The Transit Function will include the Identity headers in outgoing signaling, and route the callback call toward the home network of the emergency caller. (See ATIS-0500032 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. As described in Clause 6.1.1, the entry point 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 “verstatValue” parameters reflecting the verification status of the Identity header associated with calling identity and the Identity header associated with the RPH. The IBCF will include the ‘verstat’ information in SIP signaling sent toward the emergency caller.

and callback calls

# Overview

In addition to caller identity authentication/verification, 9-1-1 calls and callback calls may also be subject to Resource-Priority Header (RPH) signing. In the context of 9-1-1 calls, a signed RPH received in an incoming 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 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 is appropriate. The SHAKEN model specified in ATIS-1000074 can be leveraged to cryptographically sign and verify the SIP RPH field in SIP INVITE messages associated with 9-1-1 and callback calls using the PASSporT extension defined in IETF RFC 8443, including the assertion values described in draft-ietf-stir-rph-emergency-services-01, and the associated Secure Telephone Identity (STI) protocols.

The framework specified in this standard supports a trust mechanism for SIP RPH values associated with emergency calls and callback calls crossing IP NNI boundaries. A high-level description of the RPH 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 token for the SIP RPH.

For callback calls:

1. The NG9-1-1 System Service Provider cryptographically signs the SIP RPH (unless a signed RPH is received in the SIP INVITE associated with the callback call from the PSAP) before sending the call across an IP NNI boundary to/toward the emergency caller’s home network. If the NG9-1-1 System Service Provider receives a signed RPH in a SIP INVITE from a PSAP associated with a callback call, the NG9-1-1 System Service Provider may validate a signed SIP RPH, but must transparently pass the received Identity header associated with the SIP RPH forward.
2. The emergency caller’s home Service Provider verifies the received signed PASSporT token for the SIP RPH.

## Protocol Support for SIP RPH Signing of Emergency Calls and Callback Calls

This ATIS standard uses the PASSporT “rph” extension specified in [IETF RFC 8443], the assertion values described in draft-ietf-stir-rph-emergency-services-01, and associated STIR protocols for cryptographic signing of the SIP RPH field in support of emergency service calls.

### RFC 8225: PASSporT: Personal Assertion Token

[IETF RFC 8225] 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 (PKI), 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 Personal Assertion Token (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 token. The public certificate is also used to validate the entity that signed the token, as defined in [IETF RFC 8226]. The validated claims and the validated identity of the entity signing the claims can both be used to determine the level of trust in the originating entity and their asserted SIP RPH information.

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

[IETF RFC 8224] 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]](#footnote-4) The 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.

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

[IETF RFC 8443] defines an optional extension to the PASSporT and the associated STIR 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 will involve the inclusion of a “ppt” extension with an “rph” claim in the PASSporT. Based on RFC 8443, 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 RFC 8443, 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.

### Assertion Values for a Resource Priority Header Claim in Support of Emergency Services Networks

[draft-ietf-stir-rph-emergency-services-01] adds new assertion values for the Resource Priority Header ("rph") claim defined in RFC 8443, in support of Emergency Services Networks for emergency call origination and callback. Specifically, this specification defines new assertions values for:

* "ESorig": Emergency Services call origination
* "EScallback": Emergency Services callback.

The following is an example of an "rph" claim for SIP 'Resource-Priority' header field with an "ESorig" assertion:

{

"orig":{"tn":"12155551212"},

"dest":{["uri":"urn:service:sos"]},

"iat":1443208345,

"rph":{"ESorig":["esnet,1"]}

}

The following is an example of an "rph" claim for SIP 'Resource-Priority' header field with an "EScallback" assertion:

{

"orig":{"tn":"12155551213"},

"dest":{["tn":"12155551212"]},

"iat":1443208345,

"rph":{"EScallback":["esnet,0"]}

}

After the header and claims PASSporT objects have been constructed, their signature is generated normally per the guidance in [RFC8225] using the full form of PASSporT.

## Governance Model and Certificate Management

The credentials (i.e., Certificate) used to create the signature must have authority over the namespace of the "rph" claim, and there is only one authority per claim. The authority MUST 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 (i.e., certificates) 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 is not within the scope of this standard.

## Reference Architecture for SIP RPH Signing

### Reference Architecture for SIP RPH Signing Associated with Emergency (9‑1‑1) Originations

Figure 1 shows the 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] and [23.228] in which an IBCF in an originating network, if configured through operator policies, invokes an AS 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 1, the emergency call is originated from service provider A’s network that performs the authentication service and is terminated in NG9-1-1 Emergency Services Network Provide 1’s network, which performs the verification service.

As described in Clause V.2.1 of 3GPP [TS 24.229], the Ms reference point is used to request the signing of an Identity header field or to request verification of a signed identity in an Identity header field. The protocol to be used on the Ms Reference Point is HTTP 1.1, as specified in [RFC 2616].



Figure – Architecture for Signing SIP RPH of Emergency Originations

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

**IMS Elements:**

* SIP User Agent (SIP UA) – This component represents the originating end point for an emergency origination.
* Proxy Session Control Function (P-CSCF) – This component receives the emergency session establishment request from the UE, detects that it is an emergency session request, and forwards it to/toward the E-CSCF.

NOTE: As specified in [TS 24.229] and [ATIS-0700015], if required by operator policy, the P-CSCF may forward the emergency session establishment request to the E-CSCF via an S-CSCF in some implementations.

* 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 forwards the call request toward 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 UE and uses that location to acquire routing information for an emergency session from the Routing Determination Function (RDF).
* Interconnection Border Control Function (IBCF) – This function is at the edge of the service provider network and represents the Network-to-Network Interface (NNI) or peering interconnection point between telephone service providers. It is the ingress and egress point for SIP calls between providers.
* 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] as an application server that performs the function of the authentication service defined in RFC 8224 in the context of caller identity authentication. 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].
* Secure Telephone Identity Verification Service (STI-VS) – Defined in [ATIS-1000074] as an application server that performs the function of the verification service defined in RFC 8224 in the context of caller identity verification. In the context of this standard, the STI-AS contains a logical component that provides the verification service for the SIP RPH signing defined in [IETF RFC 8443].
* Call Validation Treatment (CVT) – Defined in [ATIS-1000074] 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 is positively or negatively verified.
* Secure Key Store (SKS) – Defined in [ATIS-1000074] as a highly secure logical element that stores secret private key(s) for the STI-AS to access.
* Certificate Provisioning Service – Defined in [ATIS-1000074] as a logical service used to provision certificate(s) used for STI.
* Secure Telephone Identity Certificate Repository (STI-CR) – Defined in [ATIS-1000074] 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.

### Reference Architecture for SIP RPH Signing Associated with Callback Calls

Figure 2 shows the reference architecture for SIP RPH signing in the context of callback calls. The architecture used for signing the SIP RPH 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 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) 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 INVITE back from the STI-AS with two added SIP Identity header fields constructed per [RFC 8224], one associated with the caller identity and one associated with the RPH, using the IMS-based NG9-1-1 Emergency Services Network provider’s credentials as the signing authority for the PSAP telephone identity and RPH.

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 toward the entry IBCF associated with the emergency caller’s home network. The home network will perform STI verification, assuming it supports such capabilities, and present the called party (i.e., the emergency caller) with an indication of the verification status of the calling telephone number and RPH.

Note that an alternative callback architecture, if supported based on local policy, will have the exit point 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]. See [ATIS-0500032.v002] for further details.



Figure 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 2 includes the following IMS element:

* Transit Function – As described in 3GPP [TS 23.228], 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.

## SIP RPH Signing Call Flows for Emergency Calling

### SIP RPH Signing Call Flow for Emergency Originations



Figure 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, optional Attestation-Info and Origination-Id header fields, and a private header (P-header) conveying the RPH assertion value in the SIP INVITE message for use by downstream calling identity authentication and verification processes. The P-CSCF passes the SIP INVITE to the E-CSCF.
3. The E-CSCF sends the INVITE to the LRF to determine routing instructions.
4. The LRF acquires location, if required, and queries the RDF for 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 signingRequests over the Ms reference point to the STI-AS. The signingRequest associated with the caller identity includes an “attest” parameter that contains the attestation information and an “origid” parameter, populated according to local policy or based on information received by the IBCF in an Attestation-Info header and an Origination-Id header, respectively, within the SIP INVITE, as well as other PASSporT information (i.e., “orig”, “dest”, iat and origid). The signingRequest associated with the RPH will include an “rph” claim that contains an assertion of “ESorig” with the value “esnet.1”, along with the “orig”, “dest”, and “iat”.[[5]](#footnote-5) The IBCF will populate the assertion value in the signingRequest either directly based on receipt of an associated P-header in the incoming SIP INVITE message (if received) or by identifying the call as an emergency origination based on other information received in incoming signaling (e.g., an ‘sos’ service URN in the Request-URI, an RPH value of esnet.1).

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

1. The STI-AS in the originating SP (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.
2. 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 [TS 24.229].
3. 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.
4. The exit IBCF uses the identityHeader parameters in the signingResponses 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 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.

1. 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 claim for each Identity header received, as well as the “to” parameter containing the destination identity from the To header, the “from” parameter containing the asserted identity from the From or P-Asserted-Identity, and a “time” parameter based on the Date header field in the incoming request.

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

1. The terminating SP STI-VS determines the STI-CR Uniform Resource Identifier (URI) and makes an HTTPS request to the STI-CR as per [ATIS-1000074].
2. The STI-VS validates the certificate and then extracts the public key as per [ATIS-1000074]. It constructs the RFC 8224 format and uses the public key to verify the signature in the identityHeader fields, which validate the caller identity and RPH field signed by the originating service provider STI-AS.
3. 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.
4. The STI-VS returns a verificationResponse to the ingress IBCF. The verificationResponse includes “verstatValues” that contain the results of the verification processes associated with the signed caller identity and RPH.

NOTE: The “verstat” values associated with verification of the RPH, and the means for signaling that information forward in the SIP INVITE message, are for further study.

1. The ingress IBCF passes the INVITE to the I- CSCF in the NG9-1-1 Emergency Services Network.
2. The I-CSCF passes the INVITE to the pre-configured E-CSCF.
3. The E-CSCF forwards the SIP INVITE to the LRF.
4. The LRF queries the RDF using the location information received in the INVITE message and the emergency service URN (urn:service:sos). The RDF returns a route URI. In this example, the route URI is associated with an i3 PSAP that is served by the NG9-1-1 Emergency Services Network.
5. The LRF redirects the call back to the E-CSCF, passing the Route (PSAP) URI.
6. The E-CSCF generates an outgoing INVITE message, using the information received from the LRF as well as information received in the initial INVITE message, and forwards it to the (egress) IBCF.
7. The (egress) IBCF forwards the SIP INVITE to the i3 PSAP with the appropriate “verstat” values and Identity headers, and normal call processing associated with the emergency origination continues.

### SIP RPH Signing Call Flow for Callback Calls



Figure 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 message from the PSAP the entry IBCF applies general screening rules to the request, and, based on local policy, adds an Origination-Id header to the INVITE to indicate from where the request was received. It then forwards the 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.

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).

1. The STI-AS determines, through service provider-specific means, the legitimacy of the content of the caller identity and the RPH field. The STI-AS then securely requests its private key from the SKS.
2. The SKS provides the private key in the response, and the STI-AS signs and adds Identity header fields per [IETF RFC 8224].
3. The STI-AS returns the SIP INVITE which includes a signed Identity header field value for the caller identity and a signed Identity header field value for the RPH in JSON objects.
4. The Transit Function routes the SIP INVITE (with the Identity headers) over the NNI using standard inter-domain routing resolution to the egress IBCF. If, based on local policy, a verstat is present in the SIP INVITE received by the Transit Function, the IBCF will remove the verstat before forwarding the call to the next network.
5. In this example, the egress 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.
6. The emergency caller’s home service provider (Service Provider A) entry IBCF initiates a verificationRequest to the STI-VS that includes an identityHeader parameter associated with the caller identity and an identityHeader parameter associated with the RPH.

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

1. The terminating SP STI-VS uses the “x5u” field in the PASSporT Protected Header per RFC 8225 to determine the STI-CR Uniform Resource Identifier (URI) and makes an HTTPS request to the STI-CR.
2. The STI-VS validates the certificate and then extracts the public key as per [ATIS-1000074]. It constructs the RFC 8224 format and uses the public key to verify the signature in the Identity header fields, which validates the caller identity and RPH field content used when the caller identity and RPH content were signed by the STI-AS.
3. 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.
4. Depending on the result of the STI validation, the STI-VS includes an appropriate indicator (that may be defined outside of this document) and returns a verificationResponse containing verstatValues to the IBCF.

NOTE: The “verstat” values associated with verification of the RPH, and the means for signaling that information forward in the SIP INVITE message, are for further study.

1. The IBCF continues to set up the callback call to the CSCF.
2. The CSCF continues to set up the callback call toward the emergency caller.
3. The terminating SIP UA receives the INVITE and normal SIP processing of the call continues, returning “200 OK” or optionally setting up media end-to-end.

# Procedures for SIP RPH Signing

This 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 field in the context of emergency calling.

## Procedures at the IBCF

The IBCF shall adhere to Clauses 4 and 5.10 in 3GPP [TS 24.229] 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 the NG9-1-1 Emergency Services Network. For emergency originations there will also be an exit point 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 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.

### Entry Point IBCF

For emergency (9-1-1) originations, the entry point 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, when receiving an initial INVITE request containing one or more SIP Identity header fields, the IBCF shall determine the originating identity to be verified by decoding the Identity header field containing a PASSporT SHAKEN JSON Web Token. While not yet addressed in TS 24.229, the IBCF shall also determine the RPH value to be verified by decoding the Identity header associated with the signed RPH. The IBCF will then build and send a verificationRequest to the STI-VS over 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 will 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 must remove it. The entry IBCF will also populate the verstat value associated with the RPH in the outgoing SIP INVITE message, based on the associated verstatValue returned in the verificationResponse. How the “verstatValue” reflecting the verification status of the Identity header associated with the signed RPH is populated in the outgoing SIP INVITE is for further study.

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

For callback calls, the entry point 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 point IBCF contains a verstat parameter in the From or P-Asserted-Identity header, the entry IBCF must 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 must add a Resource-Priority header set to “esnet.0” (if not already present) to the SIP INVITE message associated with the callback call. Based on local policy, the entry point IBCF may also add an Origination-Id header to the SIP INVITE, indicating from where the request was received.

For callback calls, the entry point 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, the entry point IBCF in the emergency caller’s home network will build and send a verificationRequest to the STI-VS over 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 will 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. The entry IBCF will also populate the verstat value associated with the RPH in the forwarded SIP request, based on the associated verstatValue returned in the verificationResponse. How the verification status of the Identity header associated with the signed RPH is populated in the outgoing SIP INVITE is for further study.

### Exit Point IBCF

For an emergency (9-1-1) origination, the exit point IBCF in the Originating Service Provider network will 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 point IBCF sends an HTTP POST containing two signingRequests 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 will include an “rph” claim as described in [RFC 8443] that contains an assertion of “ESorig” as described in [draft-ietf-stir-rph-emergency-services-01] and a value of “esnet.1”, along with the “orig”, “dest”, and “iat. The exit IBCF will populate the assertion value in the signingRequest either directly based on receipt of an associated P-header in the incoming SIP INVITE message (if received) or by identifying the call as an emergency origination based on other information received in incoming signaling (e.g., an ‘sos’ service URN in the Request-URI, an RPH value of esnet.1). The exit point IBCF includes the signed Identity headers received in the HTTP signingResponses in the outgoing request. The exit point IBCF must remove the verstat from the From header or P-Asserted-Identity header prior to sending the SIP INVITE over the IP NNI to 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 point 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 NENA i3 PSAP). The IBCF shall pass all headers and message bodies unless passing of the parameters is prohibited with its role as a border gateway function.

In support of callback calls, the exit point 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 with its role as a border gateway function.

## Procedures at the STI-AS

In the context of emergency (9-1-1) originations, the STI-AS will receive an HTTP POST from the IBCF that includes a signingRequest that contains base and SHAKEN PASSporT claims (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 signingResponse messages within an HTTP 200 OK.

In the context of callback calls, the STI-AS will 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 telephone number identity and RPH being used in the INVITE. The STI-AS is then responsible for cryptographically signing the PASSporT and adding Identity header fields and signatures (corresponding the caller identity and RPH) to the SIP INVITE that it returns to the Transit Function.

## Procedures at the STI-VS

The STI-VS is an application server that performs the function of the verification service defined in RFC 8224. In the context 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. Upon receiving an HTTP verificationRequest associated with an emergency (9-1-1) origination from an entry IBCF in the NG9-1-1 Emergency Services Network (for emergency originations) or the emergency caller’s home network (for callback calls), the STI-VS retrieves the certificate referenced by the “x5u” field in the PASSporT protected header from the STI-CR. The STI-VS follows the basic certificate path processing as described in [RFC 5280], following the chain until the root is reached. The STI-VS ensures that the root certificate is on the list of trusted STI-CAs. The STI-VS validates that the PASSporT information provided in the Identity headers contained in the verificationRequest includes all of the baseline claims, as well as the SHAKEN extension claims and rph claim. The verifier shall also follow the RFC 8224-defined verification procedures to check the corresponding date, originating identity and destination identities, with the restrictions specified in ATIS-1000074. The STI-VS will return “verstatValue” parameters in the HTTP verificationResponse to convey the results of the verification. 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.

NOTE: The specific ‘verstat’ values associated with RPH signing verification success/failure are for further study.

## Procedures at the P-CSCF

A P-CSCF operating in an Originating Service Provider network that supports calling number authentication and RPH signing may, based on local policy, be responsible for inserting attestation information related to the asserted calling identity and populating the RPH in a SIP INVITE associated with an emergency origination. According to 3GPP [TS 24.229], 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], associated with the caller identity, and an optional origination identifier (in the form of a UUID) in an Origination-Id header field. The P-CSCF may also populate a value of “esnet.1” in the RPH and, also based on local policy, populate a P-header conveying the RPH assertion value in a SIP INVITE message associated with an emergency origination.

## Procedures at the Transit Function

The Transit Function (TRF) is expected to adhere to the procedures described in Clauses 4.15.3 and 5.19 of 3GPP [TS 23.228] 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 signing will 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 value 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 it 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 INVITE back from the STI-AS with an added SIP Identity header field (associated with the calling identity) constructed per RFC 8224 [36], using the IMS-based NG9-1-1 Emergency Services Network provider’s credentials as the signing authority for the PSAP telephone identity. The INVITE returned by the STI-AS will also include an Identity header associated with the RPH. After receiving the SIP INVITE from the STI-AS, the Transit Function will route the call to the exit IBCF.

1. Available from the Internet Engineering Task Force (IETF) at: < <https://www.ietf.org/> >. [↑](#footnote-ref-1)
2. This document is available from the Third Generation Partnership Project (3GPP) at:   
   < <http://www.3gpp.org/specs/specs.htm> >. [↑](#footnote-ref-2)
3. [↑](#footnote-ref-3)
4. Note that when using the Ms reference point defined in [TS 24.229] to interact with the authentication service, the authentication service will return identityHeader parameter(s) in the signingResponse and the element that sent the signingRequest (i.e., the IBCF) will be responsible for populating the Identity headers in the outgoing SIP INVITE message. [↑](#footnote-ref-4)
5. The HTTP interface used over the Ms interface needs to be enhanced to support the conveyance of the “rph” claim and associated assertion values. [↑](#footnote-ref-5)