



1200 G Street, NW
Suite 500
Washington, DC 20005

P: +1 202-628-6380
W: www.atis.org

May 21, 2021

To: Members of ATIS PTSC

Subject: Default of ATIS Letter Ballot – PTSC-LB-261, draft proposed ATIS Standard, Session Initiation Protocol (SIP) Resource-Priority Header (RPH) and Priority Header Signing in Support of Emergency Calling

Dear Members:

The results for the Letter Ballot of ATIS Letter Ballot PTSC-LB-261 were 15 approvals, 0 disapprovals, 10 abstentions, and 7 ballots were not returned.

**The results of the Letter Ballot, including the comments submitted are designated as Attachment I. The comments have been addressed by IP-NNI TF and the resolution to these comments is designated as Attachment II. A summary of how these comments were considered can be found in the following meeting notes: [May 12-13, 2021](#). The revised text of this proposed standard is designated as Attachment III.

Please review the changes made to resolve the comments. If these changes should affect your original vote or if you did not vote on the initial letter ballot and choose to vote at this time, please advise ATIS in writing by casting your vote in ATIS Workspace by **June 23, 2021**. Any vote not changed will carry forward to the current Default Letter Ballot.

Thank you for your attention to this matter.

Sincerely,

[Original signed by A. Karditzas]

Anna Karditzas
Coordinator, Global Standards Development

Attachments

ATIS Letter Ballot Comment Submittal Form and Consideration Report

All commenters should use this form when submitting comments on an ATIS Letter Ballot ([view the instructions](#)). This form should accompany the [letter ballot \(via ATIS Workspace\)](#) and will subsequently be used during comment consideration by the appropriate committee/subcommittee.

The commenter should use the “track changes” feature when recommending changes to existing text. Proposed changes to a table, figure, or any other item that is not purely text, should include a summary in the table below and provide the modified table, figure, etc., in the “Other Information” section. The source file for any new figures (Visio, PowerPoint, etc.) must also be included (by either zipping together with this document, or embedding as a file/object).

Letter Ballot: PTSC-LB-261 (PTSC-2021-00017R000)

| Company Name: Neustar | | | | | | |
|------------------------------|-------------------------|---|---|----------------------------------|-------------------|--|
| TO BE COMPLETED BY COMMENTER | | | | TO BE COMPLETED BY SUB/COMMITTEE | | |
| Auto# | Page/ Section/Line # | Comment | Rationale/Suggested Solution | Type ¹ | Res. ² | Discussion/Explanation/Note (if comment is modified, accepted/modified via a separate ballot comment, or not accepted) |
| 1 | Abstract | Remove extraneous “header” | Remove | | | |
| 2 | Line 9, 281 | Consistent use of “header” when used with RPH | Change all to “Resource-Priority Header” to align with RPH acronym | | | |
| 3 | Line 9,126 | Consistent use of quotes/double quotes | Review and change all to preferred symbol | | | |
| 4 | Lines 14-15 | “trust domain implementation is set to remove it if it occurs from the UE”? | Change to “trust domain implementation removes it if set by the UE” | | | |
| 5 | Lines 14-15, 363, 378 | Seems like preferred term is User Agent or UA? | If so and these terms are equivalent, change “User Equipment” to “User Agent” and “UE” to “UA” throughout | | | |
| 6 | Line 47 | “caller identity authentication and verification”, I assume, is SHAKEN? | If so, consider changing to, “caller identity (SHAKEN) authentication and | | | |

¹ Type of change: Insert **S** or **NS**: Substantive (**S**) (see [ATIS OP Section A.6](#)) or Non-Substantive (**NS**)

² Resolution (how was comment considered): Insert **A**, **AM**, **N**, **I**, or **W**: Accepted (**A**), Accepted as Modified (**AM**), Not Accepted (**N**), For Information/No Action/Noted (**I**), or Withdrawn (**W**).

ATIS Letter Ballot Comment Submittal Form and Consideration Report

| | | | | | | |
|----|---------------|---|--|--|--|--|
| | | | verification” to avoid any confusion and since used throughout document | | | |
| 7 | Lines 50-51 | “The display of information associated with the verification of SIP RPH and Priority header values is also outside the scope of this document.” | Consider changing to, “Finally, the display of information associated with the verification of SIP RPH and Priority header values is outside the scope of this document | | | |
| 8 | Line 126 | Consistent use of double quotes. One example, but should be checked throughout document | Change ‘esnet’ to “esnet” | | | |
| 9 | Line 105 | “9-1-1” is not really a 3 digit code | Consider changing all to “911” except for “NG9-1-1” | | | |
| 10 | Line 143 | “is trusted” | Change to “can be trusted” | | | |
| 11 | Line 147 | “signing verification” | To avoid confusion, consider changing to just “verification” – OK with also removing note as proposed by editor | | | |
| 12 | Line 151 | Extraneous “terminating” | Delete | | | |
| 13 | Lines 177-178 | “attest” is required, at least for 82 API? | Not sure why optional for Ms? If so, not sure how it then complies with SHAKEN? “The PASSporT “shaken” extension shall include both an attestation indicator (“attest”), as described in section 5.2.3 and an origination identifier (“origid”) as described in section 5.2.4.” Suggestion discussed with editor was to make required in this document | | | |
| 14 | Line 185 | “will include the value of the “identity” claim in an Identity header field” | Consider changing to “will include the signingRequest response data in an Identity header field” | | | |
| 15 | Line 190 | Missing comma | Change to “caller identity, as well as” | | | |
| 16 | Line 203, 601 | Grammar | Change “toward” to “towards” | | | |

ATIS Letter Ballot Comment Submittal Form and Consideration Report

| | | | | | | |
|----|--------------------|--|--|--|--|--|
| 17 | Line 222 | Reference “originating service provider” same way | “Originating Service Provider” seems to be preferred | | | |
| 18 | Line 274 | Footnote 4 | Change “sent” to “sends” | | | |
| 19 | 279, 300, 650 | Consistent use of “Resource Priority” | Change all to “Resource-Priority” or “Resource Priority” | | | |
| 20 | Line 315 | First normative references of “shall” and “must”. However, Clause (5) is entitled “Overview”? Only a few normative references (“must” or “shall”) in this section? | If meant to be normative for this standard, then it should just be clearer to reader where such normative text is included in the document. Discussed with editor to change title and note that this Clause contains some normative text | | | |
| 21 | Line 481 | Note about AS is ambiguous | Consider adding, “processing (i.e., after routing URI has been determined)” or remove Note | | | |
| 22 | Line 506, 578, 733 | Note about VS is ambiguous | Consider adding, “processing (i.e., before routing URI is determined)” or remove Note | | | |
| 23 | Line 525 | Extraneous “forward” | Delete; OK if note removed as proposed by editor | | | |
| 24 | Line 527 | Extra space | Change to “I-CSCF” | | | |
| 25 | Line 531, 534 | Consistency | Change “route URI” to “routing URI” | | | |
| 26 | Lines 538-539 | Generally, Identity headers are stripped after STI-VS and before sending to UA? If these need to be preserved, then should better clarify this | Discussed with editor and a footnote should be adequate | | | |
| 27 | Line 552 | Why just this one (tagging) header and not an “Attestation-Info” header too as in Line 664? | Unless there is a significance, suggest that both these headers may be added per local policy | | | |

ATIS Letter Ballot Comment Submittal Form and Consideration Report

| | | | | | | |
|----|---------------|--|---|--|--|--|
| 28 | Line 598 | Extraneous comma | Change to “message is for further study.” OK, if this text is deleted as proposed by editor | | | |
| 29 | Line 606 | Clarify normative clause | Change to “This normative clause...” | | | |
| 30 | Line 706 | Grammar | Change to, “for the caller ...” | | | |
| 31 | Lines 744-745 | Remove UUID parenthetical about Origination ID since defined in ATIS-1000074 | | | | |

Other Information (e.g., Tables, Figures):

ATIS Letter Ballot Comment Submittal Form and Consideration Report

All commenters should use this form when submitting comments on an ATIS Letter Ballot ([view the instructions](#)). This form should accompany the [letter ballot \(via ATIS Workspace\)](#) and will subsequently be used during comment consideration by the appropriate committee/subcommittee.

The commenter should use the “track changes” feature when recommending changes to existing text. Proposed changes to a table, figure, or any other item that is not purely text, should include a summary in the table below and provide the modified table, figure, etc., in the “Other Information” section. The source file for any new figures (Visio, PowerPoint, etc.) must also be included (by either zipping together with this document, or embedding as a file/object).

Letter Ballot: [PTSC-LB-261]

| Company Name: [Ericsson] | | | | TO BE COMPLETED BY COMMENTER | | TO BE COMPLETED BY SUB/COMMITTEE | |
|--------------------------|----------------------------|---|--|------------------------------|-------------------|--|--|
| Auto# | Page/Section/Line # | Comment | Rationale/Suggested Solution | Type ¹ | Res. ² | Discussion/Explanation/Note (if comment is modified, accepted/modified via a separate ballot comment, or not accepted) | |
| 1 | 2/1.2/ line 61 | Reword to improve readability | Change to: against unauthorized spoofing <u>of</u> , or tampering <u>of—with</u> , the information conveyed in the SIP RPH or Priority header. This | | | | |
| 2 | 2/1.2/ line 63 | Add quotes around rph for consistency | Change to: how the PASSporT <u>“rph”</u> extension | | | | |
| 3 | 5/4.1/ lines 139-140 | Add the word “a” to improve readability | Change to: A Service Provider can use the same Secure Telephone Identity (STI) certificates for signing <u>a</u> SIP RPH/Priority header as they use for telephone number (TN) signing, but is not required to do so. | | | | |
| 4 | 5/4.1/ | The Note can be removed because | Remove the following note: | | | | |

¹ Type of change: Insert **S** or **NS**: Substantive (**S**) (see [ATIS OP Section A.6](#)) or Non-Substantive (**NS**)

² Resolution (how was comment considered): Insert **A**, **AM**, **N**, **I**, or **W**: Accepted (**A**), Accepted as Modified (**AM**), Not Accepted (**N**), For Information/No Action/Noted (**I**), or Withdrawn (**W**).

ATIS Letter Ballot Comment Submittal Form and Consideration Report

| | | | | | |
|---|----------------------|--|--|--|--|
| | lines 147-148 | 3GPP has defined a SIP header to carry the verification status associated with an RPH/Priority header | NOTE: The mechanism to convey RPH/SIP Priority header signing verification success/failure via 'verstat' in a SIP INVITE message is for further study. | | |
| 5 | 6/4.2/ line177-178 | Add quotation marks for consistency Make inclusion of "attest" claim mandatory for consistency with ATIS-1000082 (even though optional in 3GPP TS 24.229) | Change to: the signingRequest includes "orig" and "dest" claims, "iat", and "origid". The signingRequest may shall also include an "attest" parameter that identifies the relation between the service provider attesting the identity and the subscriber. | | |
| 6 | 6/4.2/ lines 212-214 | Modify to align with 3GPP agreements regarding definition of verificationResponse parameter to convey RPH/Priority header verification status | Change to: a "verstatValue" parameters 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 will include the 'verstat' verification status information in the SIP signaling sent towards the emergency caller. | | |
| 7 | 6/5/ line 218 | Make section title more explicit. | Change to: 5 <u>SIP RPH and Priority Header Authentication for 9-1-1 Overview</u> | | |
| 8 | 7/5/ lines 243-244 | Modify parenthetical expression to align with NENA i3 draft standards which describe signing of RPH and Priority header in NG9-1-1 Emergency Services Network. | Change to: (unless a signed RPH and Priority header are received in the SIP INVITE associated with the a callback call from the a PSAP) | | |
| 9 | 8/5.1.4/ Footnote #4 | Consistency in use of plural nouns | Change to: ⁴ Note that when using the Ms reference point defined in 3GPP TS 24.229 [Ref 2] to interact with the authentication | | |

ATIS Letter Ballot Comment Submittal Form and Consideration Report

| | | | | | |
|----|---|--|--|--|--|
| | | | service, the authentication service will return identityHeader parameter(s) in the signingResponse(s) and . . . | | |
| 10 | 10/5.3.1/ line 362 | Missing word “Call” in Proxy Call Session Control Function (P-CSCF) | Change to: Proxy <u>Call</u> Session Control Function (P-CSCF) | | |
| 11 | 12/5.4.1/ line 466 | Add text to clarify description of call flow step to better align with figure. | Change to: Info and Origination-Id header fields. <u>The P-CSCF forwards the SIP INVITE to the E-CSCF.</u> | | |
| 12 | 13/5.4.1/ line 479 | Delete footnote #5 since 3GPP has agreed on enhancements to Ms interface to support the conveyance of the “rph” claim and associated assertion value | Delete Footnote #5 and associated reference: “esnet.1”, along with the “orig”, “dest”, and “iat”. ⁵ ⁵The HTTP interface used over the Ms interface needs to be enhanced to support the conveyance of the “rph” claim and associated assertion values. | | |
| 13 | 13/5.4.1/ Step 12/ lines 501-502 | Modify text to align with 3GPP agreements regarding use of identityHeaders parameter to convey signed RPH information in verificationRequest | Change to: The verificationRequest includes an identityHeader claim <u>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</u> for each Identity header received , as well as the “to” parameter containing the . . . | | |
| 14 | 13/5.4.1/ Step 14/ line 512 | Modify text to align with 3GPP agreements regarding use of identityHeaders parameter to convey signed RPH information in verificationRequest | Change to: identityHeader fields <u>and identityHeaders parameters</u> , which validates the caller identity and RPH field signed by the originating service | | |

ATIS Letter Ballot Comment Submittal Form and Consideration Report

| | | | | | | |
|----|---|---|---|--|--|--|
| 15 | 13/5.4.1/ Step 16/ lines 516-525 | <p>Modify text to align with 3GPP agreements regarding the definition of a new parameter in a verificationResponse to convey RPH verification status;</p> <p>Update RPH verification status values to align with 3GPP agreements;</p> <p>Delete footnote #6;</p> <p>Delete Note</p> | <p>Change to:</p> <p>16. The STI-VS returns a verificationResponse to the ingress 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 will be set to “TN-Validation-Passed”, “TN-Validation-Failed”, or “No-TN-Validation”, and the “verstatValueverstatPriority” associated with the signed RPH will be provisionally set to “Emergency-Services-RPH-Validation-Passed”, “Emergency-Services-RPH-Validation-Failed”, or “No-Emergency-Services-RPH-Validation”.⁶</p> <p>NOTE: The value of the “verstatValue” parameter used to convey verification results associated with a signed RPH are provisional, pending final resolution in 3GPP. The means for signaling ‘verstat’ information associated with an RPH forward in the SIP INVITE message is for further study.</p> | | | |
| 16 | 14/5.4.1/ Step 17/ line 527 | <p>Add text to clarify description of call flow step to include 3GPP agreements regarding the definition of a SIP header to convey RPH/Priority header verification status information</p> | <p>Change to:</p> <p>17. The ingress 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</p> | | | |

ATIS Letter Ballot Comment Submittal Form and Consideration Report

| | | | | | |
|----|---|---|--|--|--|
| | | | <p><u>the SIP INVITE, and</u> passes the SIP INVITE to the I- CSCF in the NG9-1-1 Emergency Services Network.</p> | | |
| 17 | 14/5.4.1/ Step 23/ lines 538-539 | <p>Add text to call flow step description to reflect 3GPP agreement regarding the definition of a SIP header to convey RPH/Priority header verification status information</p> <p>Add a footnote that provides justification for passing the Identity headers to the PSAP</p> | <p>Change to:</p> <p>23. The (exit) IBCF forwards the SIP INVITE to the i3 PSAP with the appropriate 'verstat' values <u>in the P-Asserted-Identity header, the Priority-Verstat header field, and the</u> Identity headers, and normal call processing associated with the emergency origination continues.^x</p> <p><u>x Delivery of the Identity headers allows PSAP call takers to use attestation level and verification status information to influence the handling of emergency calls.</u></p> | | |
| 18 | 14/5.4.2/ Step 2/ line 552-553 | <p>Consistent with 3GPP TS 24.229 add text to allow entry IBCF to add Attestation-Info header as well as Originating-Id header, based on local policy</p> | <p>Change to:</p> <p>request and, based on local policy, adds an Origination-Id header, <u>to the SIP INVITE</u> to indicate from where the request was received, <u>and an Attestation-Info header to the SIP INVITE.</u></p> | | |
| 19 | 15/5.4.2/ Step 9/ line 576-577 | <p>Update text to reflect the use of the identityHeaders parameter to convey signed RPH in a verificationRequest</p> | <p>Change to:</p> <p>verificationRequest to the STI-VS that includes an identityHeader parameter associated with the caller identity and an <u>identityHeaders</u> parameter associated with the RPH/SIP Priority header.</p> | | |
| 20 | 15/5.4.2/ Step 13/ lines 589-598 | <p>Modify text to align with 3GPP agreements regarding the definition of a new parameter in a verificationResponse to convey RPH verification status;</p> <p>Update RPH verification status values</p> | <p>Change to:</p> <p>13. Depending on the result of verification, the STI-VS includes an appropriate indicator (not defined in this document) and returns a verificationResponse containing <u>a</u> verstatValue parameter<u>s</u> <u>(associated</u></p> | | |

ATIS Letter Ballot Comment Submittal Form and Consideration Report

| | | | | | | |
|----|-----------------------------|---|--|--|--|--|
| | | <p>to align with 3GPP agreements; Delete footnote #7; Delete Note</p> | <p>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 will be set to “TN-Validation-Passed”, “TN-Validation-Failed”, or “No-TN-Validation”, and the “verstatValueverstatPriority” associated with the signed RPH/SIP Priority header will provisionally be set to “Emergency-ServicesECB-RPH-Priority-Header-Validation-Passed”, “Emergency-ServicesECB-RPH-Priority-Header-Validation-Failed”, or “No-Emergency-ServicesECB-RPH-Priority-Header-Validation”.⁷</p> <p>NOTE: The value of the “verstatValue” parameter used to convey verification results associated with a signed RPH/SIP Priority header are provisional, pending final resolution in 3GPP. The means for signaling the ‘verstat’ information associated with the RPH/SIP Priority header in the SIP INVITE message, is for further study.</p> | | | |
| 21 | 15/5.4.2/ Step 14/ line 600 | Add text to clarify description of call flow step to include 3GPP agreements regarding the definition of a SIP header to convey RPH/Priority header verification status information | <p>Change to:</p> <p>14. The IBCF <u>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.</u></p> | | | |
| 22 | 16/6.1.1/ line 623 | Remove text referencing 3GPP TS 24.229. | <p>Change to:</p> <p>While not yet addressed in 3GPP TS 24.229 [Ref 2], theThe IBCF shall also</p> | | | |

ATIS Letter Ballot Comment Submittal Form and Consideration Report

| | | | | | |
|----|-------------------------------|---|--|--|--|
| | | | determine the RPH value to be verified by | | |
| 23 | 16/6.1.1/ lines 629-632 | Update text to reflect 3GPP agreements regarding the SIP header used to convey RPH verification status. | <p>Change to:</p> <p>The entry IBCF will also populate <u>a Priority-Verstat header field</u> the 'verstat' value associated with the RPH in the outgoing SIP INVITE, based on the associated "verstatPriority" parameter<u>verstatValue</u> returned in the verificationResponse, <u>to convey the verification status of the Identity header associated with the RPH.</u> 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.</p> | | |
| 24 | 16/6.1.1/ lines 653-656 | Update text to reflect 3GPP agreements regarding the SIP header used to convey RPH verification status. | <p>Change to:</p> <p>The entry IBCF will also populate the 'verstat' value<u>verification status</u> associated with the signed RPH/SIP Priority header in <u>a Priority-Verstat header field in</u> the forwarded SIP request, based on the associated verstatValue<u>"verstatPriority" parameter</u> returned in the verificationResponse. How the verification status of the Identity header associated with the signed RPH/SIP Priority header is populated in the outgoing SIP INVITE is for further study.</p> | | |
| 25 | 17/6.2/ line 706 | Missing word | <p>Change to:</p> <p>(corresponding <u>to</u> the caller identity and RPH/SIP Priority header) to the SIP INVITE . . .</p> | | |
| 26 | 18/6.3/ line 717 | Missing word | <p>Change to:</p> <p>In the context <u>of</u> emergency calling, the STI-VS provides . . .</p> | | |

ATIS Letter Ballot Comment Submittal Form and Consideration Report

| | | | |
|----|-----------------------------|--|--|
| 27 | 18/6.3/ lines 729-731 | Update text to reflect 3GPP agreements regarding parameters in the verificationResponse and new SIP header | <p>Change to:</p> <p><u>The-If an Ms reference point is used to interact with the STI-VS, the STI-VS will return a “verstatValue” parameters (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 the–an HTTP verificationResponse. If a SIP interface is used to interact with the STI-VS, the STI-VS will return a ‘verstat’ parameters 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.</u></p> |
|----|-----------------------------|--|--|

Other Information (e.g., Tables, Figures):

ATIS Letter Ballot Comment Submittal Form and Consideration Report

All commenters should use this form when submitting comments on an ATIS Letter Ballot ([view the instructions](#)). This form should accompany the [letter ballot \(via ATIS Workspace\)](#) and will subsequently be used during comment consideration by the appropriate committee/subcommittee.

The commenter should use the “track changes” feature when recommending changes to existing text. Proposed changes to a table, figure, or any other item that is not purely text, should include a summary in the table below and provide the modified table, figure, etc., in the “Other Information” section. The source file for any new figures (Visio, PowerPoint, etc.) must also be included (by either zipping together with this document, or embedding as a file/object).

Letter Ballot: **[PTSC-LB-261]**

| Company Name: [Perspecta Labs] | | | | | | |
|---------------------------------------|---------------------|---|---------------------------------------|----------------------------------|-------------------|--|
| TO BE COMPLETED BY COMMENTER | | | | TO BE COMPLETED BY SUB/COMMITTEE | | |
| Auto# | Page/Section/Line # | Comment | Rationale/Suggested Solution | Type ¹ | Res. ² | Discussion/Explanation/Note (if comment is modified, accepted/modified via a separate ballot comment, or not accepted) |
| 1 | Abstract | “SIP RPH field” → “SIP RPH header field” | Terminology consistency | | | |
| 2 | 23 + | “RPH and Priority header” → “RPH/Priority header” | Terminology consistency | | | |
| 3 | 127 | “network” → “network,” | Improved readability | | | |
| 4 | 149 | Delete blank line | Consistent formatting | | | |
| 5 | 144, 150 | Consider breaking items 9 and 10 into separate assumptions if verstat and handling might potentially be different based on Caller ID vs. RPH validation | Increased flexibility of formulation. | | | |
| 6 | 173 + | “egress IBCF” → “exit IBCF” and “ingress IBCF” → “entry IBCF” | Terminology consistency | | | |
| 7 | 213 | Is verstat needed for RPH? It's FFS in 5.4.1 | Provide another FFS disclaimer? | | | |

¹ Type of change: Insert **S** or **NS**: Substantive (**S**) (see [ATIS OP Section A.6](#)) or Non-Substantive (**NS**)

² Resolution (how was comment considered): Insert **A**, **AM**, **N**, **I**, or **W**: Accepted (**A**), Accepted as Modified (**AM**), Not Accepted (**N**), For Information/No Action/Noted (**I**), or Withdrawn (**W**).

ATIS Letter Ballot Comment Submittal Form and Consideration Report

| | | | | | | |
|----|---------|---|---|--|--|--|
| 8 | 220 | “Resource-Priority Header (RPH)” → “RPH” | Redundant acronym definition. | | | |
| 9 | 249 | “5.1 Protocol Support for SIP RPH and Priority header Signing of Emergency Calls and Callback Calls” → “5.1 Protocol Support” | Simplification suggestion. Entire scope of the document is SIP RPH and Priority header Signing of Emergency Calls and Callback Calls. | | | |
| 10 | 266 | “can both be used to determine” → “can be used to determine” | Deleted potentially confusing word” | | | |
| 11 | 299 | “5.1.4 Assertion Values for a Resource Priority Header Claim and Specification of SIP Priority Header Claim in Support of Emergency Services Networks” → “5.1.4 Assertion Values” | Simplification suggestion. | | | |
| 12 | 313 | “Header” → “header” | Correction of typo | | | |
| 13 | 313 | Why dissimilar from RPH header field? | Provide clarification. | | | |
| 14 | 328-329 | After the PASSporT header and claims have been constructed, their signature is generated normally per the guidance in IETF RFC 8225 [Ref 14] using the full form of PASSporT. | Should this sentence include a “shall”? | | | |
| 15 | 332 + | “must” → “shall” | Consistency of terms. | | | |
| 16 | 339 | “5.3 Reference Architecture for SIP RPH and Priority Header Signing” → “5.3 Reference Architecture” | Simplification suggestion. | | | |
| 17 | 340-341 | “5.3.1 Reference Architecture for SIP RPH Signing Associated with Emergency (9-1-1) Originations” → “Emergency (9-1-1) Originations” | Simplification suggestion. | | | |
| 18 | 346 | “signing of identity information if available in an incoming request. → | Addition of commas for improved readability. | | | |

ATIS Letter Ballot Comment Submittal Form and Consideration Report

| | | | | | |
|----|-------------------------------------|--|---|--|--|
| | | “signing of identity information, if available, in an incoming request.” | | | |
| 19 | 369 | Delete blank line | Formatting consistency. | | |
| 20 | 392, 396, 398, 401, 403 | Consider deleting “logical.” It’s a given that an element can be logical or physical depending on the implementation. Not used in prior clause for IMS elements. | Simplification. | | |
| 21 | 402 | Add: “(Any element that accesses the key store (i.e., STI-AS) should also be highly secure.)” | Clarification indicating the need for highly-secure key store access. | | |
| 22 | 415 (414) | “5.3.2 Reference Architecture for SIP RPH and Priority Header Signing Associated with Callback Calls” → “5.3.2 Callback Calls” | Simplification | | |
| 23 | 438 (437) | Is this paragraph the case where the Transit Function is not configured? | Provide clarification. | | |
| 24 | 455 (454) | “5.4 SIP RPH Signing Call Flows for Emergency Calling” → “5.4 Call Flows” | Simplification | | |
| 25 | 456 (455) | “5.4.1 SIP RPH Signing Call Flow for Emergency (9-1-1) Originations” → “5.4.1 Emergency (9-1-1) Originations | Simplification. | | |
| 26 | 473-483 | Use sub-bullets as indicated. | Improved readability. | | |
| 27 | 529 (528) | Delete blank line. | Formatting consistency. | | |
| 28 | 544 (543) | “5.4.2 SIP RPH and Priority Header Signing Call Flow for Callback Calls” → “5.4.2 Callback Calls” | Simplification. | | |

ATIS Letter Ballot Comment Submittal Form and Consideration Report

| | | | | | | |
|----|----------------------|--|---|--|--|--|
| 29 | 550-551 (549-550) | “1. The PSAP Call Handling Function initiates a callback call with the callback URI from the original emergency call in the To header...” → “1. The PSAP Call Handling Function initiates a callback call with the callback URI derived from the original emergency call To header...” | Improved readability. | | | |
| 30 | 563 (560) | Delete blank line. | Formatting consistency. | | | |
| 31 | 571-572 (568-569) | “7. The Transit Function routes the SIP INVITE (with the Identity headers) over the NNI using standard inter-domain routing resolution to the egress IBCF.” → “The Transit Function routes the SIP INVITE (with the Identity headers) to the exit IBCF using standard inter-domain routing resolution. | Improved accuracy and readability. | | | |
| 32 | 583 (579) | Delete blank line. | Formatting consistency. | | | |
| 33 | 594-595 (589-590) | “the STI-VS includes an appropriate indicator (not defined in this document)...” → “the STI-VS includes an appropriate indicator of the verification result (defined in [Ref 2])...” | Added reference. Improved readability. | | | |
| 34 | 605 (600) | “14. The IBCF continues to set up the callback call to the CSCF.” → “The IBCF receives the response from the STI-VS, decides what to do based on local policy, sets the verstat in the SIP message, etc. and forwards the SIP INVITE.” | Suggestion for providing additional detail. | | | |

ATIS Letter Ballot Comment Submittal Form and Consideration Report

| | | | | | | |
|----|-------------------------------|--|---|--|--|--|
| 35 | 606 (601) | “15. The CSCF continues to set up the callback call toward the emergency caller.” → “The CSCF strips the RPH header and forwards the SIP INVITE to the emergency caller.” | Suggestion for providing additional detail. | | | |
| 36 | 630 + (625 +) | “assuming the Ms reference point.” → “via the Ms reference point” | Clearer wording. | | | |
| 37 | 643 + (638 +) | “entry point IBCF” vs. “entry IBCF” | Need consistent terminology throughout? | | | |
| 38 | 644 (639) | “and once the message is validated,” | Clarify how it validates the message, since Caller ID and RPH have not yet been signed. | | | |
| 39 | 657 (652) | “this parameter” → “the “verstatValue” parameter” | Clarification. | | | |
| 40 | 660 (655) | “based on the associated verstatValue returned” → “based on the associated “verstatValue” parameter returned” | Clearer wording. | | | |
| 41 | 676 (670) | “The exit point IBCF must remove the ‘verstat’ from the From header...” → The exit point IBCF must remove the ‘verstat’, if any, from the From header | Clarification. | | | |
| 42 | 726 – 731 (720- 725) | “Assuming the Ms reference point, upon receiving an HTTP verificationRequest associated with an emergency (9-1-1) origination from an entry IBCF in the IMS NG9-1-1 Emergency Services Network (for emergency originations), or an HTTP verificationRequest or SIP INVITE from 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 can receive a verification request in one of | Improved readability. | | | |

ATIS Letter Ballot Comment Submittal Form and Consideration Report

| | | | | | |
|----|----------------------|---|---|--|--|
| | | two ways: by receiving an HTTP verificationRequest associated with an emergency (9-1-1) origination via the Ms reference point from an entry IBCF in the IMS NG9-1-1 Emergency Services Network (for emergency originations), or receipt an HTTP verificationRequest or by receiving a SIP INVITE from 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, and follows the basic certificate path..." | | | |
| 43 | 736-737 (728-729) | "The verifier shall also follow the IETF RFC 8224-defined [Ref 13] verification procedures" → "The verifier shall also follow the verification procedures defined in IETF RFC 8224 [Ref 13]" | Improved readability. | | |
| 44 | 753-754 (744-745) | Add reference at end of sentence? | Clarification. | | |
| 45 | 754-755 (745-746) | "The P-CSCF may also populate a value of "esnet.1" in the RPH." | If the P-CSCF is doing the signing for emergency calls, should this be a "shall"? | | |

Other Information (e.g., Tables, Figures):

ATIS Letter Ballot Comment Submittal Form and Consideration Report

All commenters should use this form when submitting comments on an ATIS Letter Ballot ([view the instructions](#)). This form should accompany the [letter ballot \(via ATIS Workspace\)](#) and will subsequently be used during comment consideration by the appropriate committee/subcommittee.

The commenter should use the “track changes” feature when recommending changes to existing text. Proposed changes to a table, figure, or any other item that is not purely text, should include a summary in the table below and provide the modified table, figure, etc., in the “Other Information” section. The source file for any new figures (Visio, PowerPoint, etc.) must also be included (by either zipping together with this document, or embedding as a file/object).

Letter Ballot: PTSC-LB-261 (PTSC-2021-00017R000)

| Company Name: Neustar | | | | | | |
|------------------------------|-------------------------|---|---|----------------------------------|-------------------|--|
| TO BE COMPLETED BY COMMENTER | | | | TO BE COMPLETED BY SUB/COMMITTEE | | |
| Auto# | Page/ Section/Line # | Comment | Rationale/Suggested Solution | Type ¹ | Res. ² | Discussion/Explanation/Note (if comment is modified, accepted/modified via a separate ballot comment, or not accepted) |
| 1 | Abstract | Remove extraneous “header” | Remove | N S | A | |
| 2 | Line 9, 281 | Consistent use of “header” when used with RPH | Change all to “Resource-Priority Header” to align with RPH acronym | N S | A | |
| 3 | Line 9,126 | Consistent use of quotes/double quotes | Review and change all to preferred symbol | N S | A | |
| 4 | Lines 14-15 | “trust domain implementation is set to remove it if it occurs from the UE”? | Change to “trust domain implementation removes it if set by the UE” | N S | A | |
| 5 | Lines 14-15, 363, 378 | Seems like preferred term is User Agent or UA? | If so and these terms are equivalent, change “User Equipment” to “User Agent” and “UE” to “UA” throughout | N S | A | |

¹ Type of change: Insert **S** or **NS**: Substantive (**S**) (see [ATIS OP Section A.6](#)) or Non-Substantive (**NS**)

² Resolution (how was comment considered): Insert **A**, **AM**, **N**, **I**, or **W**: Accepted (**A**), Accepted as Modified (**AM**), Not Accepted (**N**), For Information/No Action/Noted (**I**), or Withdrawn (**W**).

ATIS Letter Ballot Comment Submittal Form and Consideration Report

| | | | | | | |
|----|---------------|---|--|--------|--------|---|
| 6 | Line 47 | “caller identity authentication and verification”, I assume, is SHAKEN? | If so, consider changing to, “caller identity (SHAKEN) authentication and verification” to avoid any confusion and since used throughout document | N S | A | |
| 7 | Lines 50-51 | “The display of information associated with the verification of SIP RPH and Priority header values is also outside the scope of this document.” | Consider changing to, “Finally, the display of information associated with the verification of SIP RPH and Priority header values is outside the scope of this document | N S | A | |
| 8 | Line 126 | Consistent use of double quotes. One example, but should be checked throughout document | Change ‘esnet’ to “esnet” | N S | A | |
| 9 | Line 105 | “9-1-1” is not really a 3 digit code | Consider changing all to “911” except for “NG9-1-1” | N S | A | |
| 10 | Line 143 | “is trusted” | Change to “can be trusted” | N S | A | |
| 11 | Line 147 | “signing verification” | To avoid confusion, consider changing to just “verification” – OK with also removing note as proposed by editor | N S | A | |
| 12 | Line 151 | Extraneous “terminating” | Delete | N S | A | |
| 13 | Lines 177-178 | “attest” is required, at least for 82 API? | Not sure why optional for Ms? If so, not sure how it then complies with SHAKEN? “The PASSporT “shaken” extension shall include both an attestation indicator (“attest”), as described in section 5.2.3 and an origination identifier (“origid”) as described in section 5.2.4.” Suggestion discussed with editor was to make required in this document | S | A M | References to ATIS-1000082 will be removed, in line with TS 24.229. |

ATIS Letter Ballot Comment Submittal Form and Consideration Report

| | | | | | | |
|----|---------------------------------------|--|--|--------|--------|--------------------------------------|
| 14 | Line 185 | “will include the value of the “identity” claim in an Identity header field” | Consider changing to “will include the signingRequest response data in an Identity header field” | N S | A | |
| 15 | Line 190 | Missing comma | Change to “caller identity, as well as” | N S | A | |
| 16 | Line 203, 601 | Grammar | Change “toward” to “towards” | N S | A | |
| 17 | Line 222 | Reference “originating service provider” same way | “Originating Service Provider” seems to be preferred | N S | A | |
| 18 | Line 274 | Footnote 4 | Change “sent” to “sends” | N S | A | |
| 19 | 279, 300, 650 | Consistent use of “Resource Priority” | Change all to “Resource-Priority” or “Resource Priority” | N S | A | |
| 20 | Line 315 | First normative references of “shall” and “must”. However, Clause (5) is entitled “Overview”? Only a few normative references (“must” or “shall”) in this section? | If meant to be normative for this standard, then it should just be clearer to reader where such normative text is included in the document. Discussed with editor to change title and note that this Clause contains some normative text | N S | A | |
| 21 | Line 481 | Note about AS is ambiguous | Consider adding, “processing (i.e., after routing URI has been determined)” or remove Note | N S | A M | i.e. changed to e.g. |
| 22 | Line 506, 578, 733763 | Note about VS is ambiguous | Consider adding, “processing (i.e., before routing URI is determined)” or remove Note | N S | A M | i.e. changed to e.g. |
| 23 | Line 525 | Extraneous “forward” | Delete; OK if note removed as proposed by editor | N S | A | |
| 24 | Line 527 | Extra space | Change to “I-CSCF” | N S | A | |

ATIS Letter Ballot Comment Submittal Form and Consideration Report

| | | | | | | |
|----|---------------|--|---|--------|---|--|
| 25 | Line 531, 534 | Consistency | Change “route URI” to “routing URI” | N S | A | |
| 26 | Lines 538-539 | Generally, Identity headers are stripped after STI-VS and before sending to UA? If these need to be preserved, then should better clarify this | Discussed with editor and a footnote should be adequate | N S | A | |
| 27 | Line 552 | Why just this one (tagging) header and not an “Attestation-Info” header too as in Line 664? | Unless there is a significance, suggest that both these headers may be added per local policy | N S | A | |
| 28 | Line 598 | Extraneous comma | Change to “message is for further study.” OK, if this text is deleted as proposed by editor | N S | A | |
| 29 | Line 606 | Clarify normative clause | Change to “This normative clause...” | N S | A | |
| 30 | Line 706 | Grammar | Change to, “for the caller ...” | N S | A | |
| 31 | Lines 744-745 | Remove UUID parenthetical about Origination ID since defined in ATIS-1000074 | | N S | A | |

Other Information (e.g., Tables, Figures):

ATIS Letter Ballot Comment Submittal Form and Consideration Report

All commenters should use this form when submitting comments on an ATIS Letter Ballot ([view the instructions](#)). This form should accompany the [letter ballot \(via ATIS Workspace\)](#) and will subsequently be used during comment consideration by the appropriate committee/subcommittee.

The commenter should use the “track changes” feature when recommending changes to existing text. Proposed changes to a table, figure, or any other item that is not purely text, should include a summary in the table below and provide the modified table, figure, etc., in the “Other Information” section. The source file for any new figures (Visio, PowerPoint, etc.) must also be included (by either zipping together with this document, or embedding as a file/object).

Letter Ballot: [PTSC-LB-261]

| Company Name: [Ericsson] | | | | TO BE COMPLETED BY COMMENTER | | TO BE COMPLETED BY SUB/COMMITTEE | |
|--------------------------|----------------------------|---|--|------------------------------|-------------------|--|--|
| Auto# | Page/ Section/ Line # | Comment | Rationale/Suggested Solution | Type ¹ | Res. ² | Discussion/Explanation/Note (if comment is modified, accepted/modified via a separate ballot comment, or not accepted) | |
| 1 | 2/1.2/ line 61 | Reword to improve readability | Change to: against unauthorized spoofing <u>of</u> , or tampering <u>of</u> with the information conveyed in the SIP RPH or Priority header. This | N S | A | | |
| 2 | 2/1.2/ line 63 | Add quotes around rph for consistency | Change to: how the PASSporT “ <u>rph</u> ” extension | N S | A | | |
| 3 | 5/4.1/ lines 139-140 | Add the word “a” to improve readability | Change to: A Service Provider can use the same Secure Telephone Identity (STI) certificates for signing <u>a</u> SIP RPH/Priority header as they use for telephone number (TN) signing, but is not required to do so. | N S | A | | |
| 4 | 5/4.1/ | The Note can be removed because | Remove the following note: | N | A | | |

¹ Type of change: Insert **S** or **NS**: Substantive (**S**) (see [ATIS OP Section A.6](#)) or Non-Substantive (**NS**)

² Resolution (how was comment considered): Insert **A**, **AM**, **N**, **I**, or **W**: Accepted (**A**), Accepted as Modified (**AM**), Not Accepted (**N**), For Information/No Action/Noted (**I**), or Withdrawn (**W**).

ATIS Letter Ballot Comment Submittal Form and Consideration Report

| | | | | | | |
|---|----------------------|--|--|--------|--------|--|
| | lines 147-148 | 3GPP has defined a SIP header to carry the verification status associated with an RPH/Priority header | NOTE: The mechanism to convey RPH/SIP Priority header signing verification success/failure via 'verstat' in a SIP INVITE message is for further study. | S | | |
| 5 | 6/4.2/ line177-178 | Add quotation marks for consistency Make inclusion of "attest" claim mandatory for consistency with ATIS-1000082 (even though optional in 3GPP TS 24.229) | Change to: the signingRequest includes "orig" and "dest" claims, "iat", and "origid". The signingRequest may shall also include an "attest" parameter that identifies the relation between the service provider attesting the identity and the subscriber. | S | N | Addressed per Neustar comment: change of "may" to "shall" rejected, and reference to ATIS-1000082 removed. |
| 6 | 6/4.2/ lines 212-214 | Modify to align with 3GPP agreements regarding definition of verificationResponse parameter to convey RPH/Priority header verification status | Change to: a "verstatValue" parameters 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 will shall include the 'verstat' verification status information in the SIP signaling sent towards the emergency caller. | S | A M | "The IBCF will..." was changed to "The IBCF shall..." |
| 7 | 6/5/ line 218 | Make section title more explicit. | Change to: 5 <u>SIP RPH and Priority Header Authentication for 9-1-1 Overview</u> | N S | A | |
| 8 | 7/5/ lines 243-244 | Modify parenthetical expression to align with NENA i3 draft standards which describe signing of RPH and Priority header in NG9-1-1 Emergency Services Network. | Change to: (unless a signed RPH and Priority header are received in the SIP INVITE associated with the a callback call from the a PSAP) | N S | A | |
| 9 | 8/5.1.4/ Footnote #4 | Consistency in use of plural nouns | Change to: ⁴ Note that when using the Ms reference point defined in 3GPP TS 24.229 [Ref 2] to interact with the authentication | N S | A | |

ATIS Letter Ballot Comment Submittal Form and Consideration Report

| | | | | | | |
|----|---|--|--|--------|---|--|
| | | | service, the authentication service will return identityHeader parameter(s) in the signingResponse(s) and . . . | | | |
| 10 | 10/5.3.1/ line 362 | Missing word “Call” in Proxy Call Session Control Function (P-CSCF) | Change to: Proxy <u>Call</u> Session Control Function (P-CSCF) | N S | A | |
| 11 | 12/5.4.1/ line 466 | Add text to clarify description of call flow step to better align with figure. | Change to: Info and Origination-Id header fields. <u>The P-CSCF forwards the SIP INVITE to the E-CSCF.</u> | N S | A | |
| 12 | 13/5.4.1/ line 479 | Delete footnote #5 since 3GPP has agreed on enhancements to Ms interface to support the conveyance of the “rph” claim and associated assertion value | Delete Footnote #5 and associated reference: “esnet.1”, along with the “orig”, “dest”, and “iat”. ⁵ ⁵The HTTP interface used over the Ms interface needs to be enhanced to support the conveyance of the “rph” claim and associated assertion values. | N S | A | |
| 13 | 13/5.4.1/ Step 12/ lines 501-502 | Modify text to align with 3GPP agreements regarding use of identityHeaders parameter to convey signed RPH information in verificationRequest | Change to: The verificationRequest includes an identityHeader claim <u>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</u> for each Identity header received , as well as the “to” parameter containing the . . . | S | A | |
| 14 | 13/5.4.1/ Step 14/ line 512 | Modify text to align with 3GPP agreements regarding use of identityHeaders parameter to convey signed RPH information in verificationRequest | Change to: identityHeader fields <u>and identityHeaders parameters</u> , which validates the caller identity and RPH field signed by the originating service | S | A | |

ATIS Letter Ballot Comment Submittal Form and Consideration Report

| | | | | | | |
|----|---|---|--|---|--------|--|
| 15 | 13/5.4.1/ Step 16/ lines 516-525 | <p>Modify text to align with 3GPP agreements regarding the definition of a new parameter in a verificationResponse to convey RPH verification status;</p> <p>Update RPH verification status values to align with 3GPP agreements;</p> <p>Delete footnote #6;</p> <p>Delete Note</p> | <p>Change to:</p> <p>16. The STI-VS returns a verificationResponse to the ingress 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 will shall be set to “TN-Validation-Passed”, “TN-Validation-Failed”, or “No-TN-Validation”, and the “verstatValueverstatPriority” associated with the signed RPH will shall be provisionally set to “Emergency-Services-RPH-Validation-Passed”, “Emergency-Services-RPH-Validation-Failed”, or “No-Emergency-Services-RPH-Validation”.⁶</p> <p>NOTE: The value of the “verstatValue” parameter used to convey verification results associated with a signed RPH are provisional, pending final resolution in 3GPP. The means for signaling ‘verstat’ information associated with an RPH forward in the SIP INVITE message is for further study.</p> | S | A M | two instances of “will” changed to “shall” |
| 16 | 14/5.4.1/ Step 17/ line 527 | <p>Add text to clarify description of call flow step to include 3GPP agreements regarding the definition of a SIP header to convey RPH/Priority header verification status information</p> | <p>Change to:</p> <p>17. The ingress IBCF <u>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</u></p> | S | A | |

ATIS Letter Ballot Comment Submittal Form and Consideration Report

| | | | | | | |
|----|---|---|--|--------|---|--|
| | | | <p><u>the SIP INVITE, and</u> passes the SIP INVITE to the I- CSCF in the NG9-1-1 Emergency Services Network.</p> | | | |
| 17 | 14/5.4.1/ Step 23/ lines 538-539 | <p>Add text to call flow step description to reflect 3GPP agreement regarding the definition of a SIP header to convey RPH/Priority header verification status information</p> <p>Add a footnote that provides justification for passing the Identity headers to the PSAP</p> | <p>Change to:</p> <p>23. The (exit) IBCF forwards the SIP INVITE to the i3 PSAP with the appropriate 'verstat' values <u>in the P-Asserted-Identity header, the Priority-Verstat header field, and the</u> Identity headers, and normal call processing associated with the emergency origination continues.^x</p> <p><u>x Delivery of the Identity headers allows PSAP call takers to use attestation level and verification status information to influence the handling of emergency calls.</u></p> | S | A | |
| 18 | 14/5.4.2/ Step 2/ line 552-553 | <p>Consistent with 3GPP TS 24.229 add text to allow entry IBCF to add Attestation-Info header as well as Originating-Id header, based on local policy</p> | <p>Change to:</p> <p>request and, based on local policy, adds an Origination-Id header, <u>to the SIP INVITE</u> to indicate from where the request was received, <u>and an Attestation-Info header to the SIP INVITE.</u></p> | N S | A | |
| 19 | 15/5.4.2/ Step 9/ line 576-577 | <p>Update text to reflect the use of the identityHeaders parameter to convey signed RPH in a verificationRequest</p> | <p>Change to:</p> <p>verificationRequest to the STI-VS that includes an identityHeader parameter associated with the caller identity and an <u>identityHeaders</u> parameter associated with the RPH/SIP Priority header.</p> | N S | A | |
| 20 | 15/5.4.2/ Step 13/ lines 589-598 | <p>Modify text to align with 3GPP agreements regarding the definition of a new parameter in a verificationResponse to convey RPH verification status;</p> <p>Update RPH verification status values</p> | <p>Change to:</p> <p>13. Depending on the result of verification, the STI-VS includes an appropriate indicator (not defined in this document) and returns a verificationResponse containing <u>a</u> verstatValue parameters <u>(associated</u></p> | S | A | |

ATIS Letter Ballot Comment Submittal Form and Consideration Report

| | | | | | | |
|----|-----------------------------------|---|--|--------|---|--|
| | | <p>to align with 3GPP agreements; Delete footnote #7; Delete Note</p> | <p>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 will-shall be set to “TN-Validation-Passed”, “TN-Validation-Failed”, or “No-TN-Validation”, and the “verstatValueverstatPriority” associated with the signed RPH/SIP Priority header will-shall <u>provisionally</u> be set to “Emergency-ServicesECB-RPH-Priority-Header-Validation-Passed”, “Emergency-ServicesECB-RPH-Priority-Header-Validation-Failed”, or “No-Emergency-ServicesECB-RPH-Priority-Header-Validation”.⁷</p> <p>NOTE: The value of the “verstatValue” parameter used to convey verification results associated with a signed RPH/SIP Priority header are provisional, pending final resolution in 3GPP. The means for signaling the ‘verstat’ information associated with the RPH/SIP Priority header in the SIP INVITE message, is for further study.</p> | | | |
| 21 | 15/5.4.2/ Step 14/ line 600 | Add text to clarify description of call flow step to include 3GPP agreements regarding the definition of a SIP header to convey RPH/Priority header verification status information | <p>Change to:</p> <p>14. The IBCF <u>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.</u></p> | S | A | |
| 22 | 16/6.1.1/ line 623 | Remove text referencing 3GPP TS 24.229. | <p>Change to:</p> <p>While not yet addressed in 3GPP TS 24.229 [Ref 2], the <u>The</u> IBCF shall also</p> | N S | A | |

ATIS Letter Ballot Comment Submittal Form and Consideration Report

| | | | | | | |
|----|-------------------------------|---|---|--------|---|--|
| | | | determine the RPH value to be verified by | | | |
| 23 | 16/6.1.1/ lines 629-632 | Update text to reflect 3GPP agreements regarding the SIP header used to convey RPH verification status. | <p>Change to:</p> <p>The entry IBCF will also populate <u>a Priority-Verstat header field</u> the 'verstat' value associated with the RPH in the outgoing SIP INVITE, based on the associated <u>"verstatPriority" parameter</u> verstatValue returned in the verificationResponse, <u>to convey the verification status of the Identity header associated with the RPH.</u> 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.</p> | S | A | |
| 24 | 16/6.1.1/ lines 653-656 | Update text to reflect 3GPP agreements regarding the SIP header used to convey RPH verification status. | <p>Change to:</p> <p>The entry IBCF will also populate the <u>'verstat' value</u> verification status associated with the signed RPH/SIP Priority header in <u>a Priority-Verstat header field in</u> the forwarded SIP request, based on the associated <u>verstatValue</u> "verstatPriority" parameter returned in the verificationResponse. How the verification status of the Identity header associated with the signed RPH/SIP Priority header is populated in the outgoing SIP INVITE is for further study.</p> | S | A | |
| 25 | 17/6.2/ line 706 | Missing word | <p>Change to:</p> <p>(corresponding <u>to</u> the caller identity and RPH/SIP Priority header) to the SIP INVITE . . .</p> | N S | A | |
| 26 | 18/6.3/ line 717 | Missing word | <p>Change to:</p> <p>In the context <u>of</u> emergency calling, the STI-VS provides . . .</p> | N S | A | |

ATIS Letter Ballot Comment Submittal Form and Consideration Report

| | | | | | | |
|----|-----------------------------|--|--|---|---|--|
| 27 | 18/6.3/ lines 729-731 | Update text to reflect 3GPP agreements regarding parameters in the verificationResponse and new SIP header | <p>Change to:</p> <p><u>The-If an Ms reference point is used to interact with the STI-VS, the STI-VS will return_a “verstatValue” parameters (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 the_an HTTP verificationResponse. If a SIP interface is used to interact with the STI-VS, the STI-VS will return a ‘verstat’ parameters 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.</u></p> | S | A | |
|----|-----------------------------|--|--|---|---|--|

Other Information (e.g., Tables, Figures):

ATIS Letter Ballot Comment Submittal Form and Consideration Report

All commenters should use this form when submitting comments on an ATIS Letter Ballot ([view the instructions](#)). This form should accompany the [letter ballot \(via ATIS Workspace\)](#) and will subsequently be used during comment consideration by the appropriate committee/subcommittee.

The commenter should use the “track changes” feature when recommending changes to existing text. Proposed changes to a table, figure, or any other item that is not purely text, should include a summary in the table below and provide the modified table, figure, etc., in the “Other Information” section. The source file for any new figures (Visio, PowerPoint, etc.) must also be included (by either zipping together with this document, or embedding as a file/object).

Letter Ballot: **[PTSC-LB-261]**

| Company Name: [Perspecta Labs] | | | | | | |
|---------------------------------------|---------------------|---|---------------------------------------|----------------------------------|-------------------|--|
| TO BE COMPLETED BY COMMENTER | | | | TO BE COMPLETED BY SUB/COMMITTEE | | |
| Auto# | Page/Section/Line # | Comment | Rationale/Suggested Solution | Type ¹ | Res. ² | Discussion/Explanation/Note (if comment is modified, accepted/modified via a separate ballot comment, or not accepted) |
| 1 | Abstract | “SIP RPH field” → “SIP RPH header field” | Terminology consistency | N S | N | |
| 2 | 23 + | “RPH and Priority header” → “RPH/Priority header” | Terminology consistency | N S | N | |
| 3 | 127 | “network” → “network,” | Improved readability | N S | A | |
| 4 | 149 | Delete blank line | Consistent formatting | N S | N | |
| 5 | 144, 150 | Consider breaking items 9 and 10 into separate assumptions if verstat and handling might potentially be different based on Caller ID vs. RPH validation | Increased flexibility of formulation. | N S | N | |
| 6 | 173 + | “egress IBCF” → “exit IBCF” and “ingress IBCF” → “entry IBCF” | Terminology consistency | N S | A | |

¹ Type of change: Insert **S** or **NS**: Substantive (**S**) (see [ATIS OP Section A.6](#)) or Non-Substantive (**NS**)

² Resolution (how was comment considered): Insert **A**, **AM**, **N**, **I**, or **W**: Accepted (**A**), Accepted as Modified (**AM**), Not Accepted (**N**), For Information/No Action/Noted (**I**), or Withdrawn (**W**).

ATIS Letter Ballot Comment Submittal Form and Consideration Report

| | | | | | | |
|----|---------|---|---|--------|---|--|
| 7 | 213 | Is verstat needed for RPH? It's FFS in 5.4.1 | Provide another FFS disclaimer? | N S | N | Superceded by Ericsson comments that address 3GPP alignment |
| 8 | 220 | “Resource-Priority Header (RPH)” → “RPH” | Redundant acronym definition. | N S | A | |
| 9 | 249 | “5.1 Protocol Support for SIP RPH and Priority header Signing of Emergency Calls and Callback Calls” → “5.1 Protocol Support” | Simplification suggestion. Entire scope of the document is SIP RPH and Priority header Signing of Emergency Calls and Callback Calls. | N S | A | |
| 10 | 266 | “can both be used to determine” → “can be used to determine” | Deleted potentially confusing word” | N S | A | |
| 11 | 299 | “5.1.4 Assertion Values for a Resource Priority Header Claim and Specification of SIP Priority Header Claim in Support of Emergency Services Networks” → “5.1.4 Assertion Values” | Simplification suggestion. | N S | A | |
| 12 | 313 | “Header” → “header” | Correction of typo | N S | A | |
| 13 | 313 | Why dissimilar from RPH header field? | Provide clarification. | N S | A | |
| 14 | 328-329 | After the PASSporT header and claims have been constructed, their signature is generated normally per the guidance in IETF RFC 8225 [Ref 14] using the full form of PASSporT. | Should this sentence include a “shall”? | S | A | After the PASSporT header and claims have been constructed, their signature <u>shall be</u> generated normally per the guidance in IETF RFC 8225 [Ref 14] using the full form of PASSporT. |
| 15 | 332 + | “must” → “shall” | Consistency of terms. | S | A | |
| 16 | 339 | “5.3 Reference Architecture for SIP RPH and Priority Header Signing” → “5.3 Reference Architecture” | Simplification suggestion. | N S | A | |
| 17 | 340-341 | “5.3.1 Reference Architecture for SIP RPH Signing Associated with | Simplification suggestion. | N S | A | |

ATIS Letter Ballot Comment Submittal Form and Consideration Report

| | | | | | | |
|----|-------------------------------------|--|---|--------|--------|---|
| | | Emergency (9-1-1) Originations” → “Emergency (9-1-1) Originations” | | | | |
| 18 | 346 | “signing of identity information if available in an incoming request. → “signing of identity information, if available, in an incoming request.” | Addition of commas for improved readability. | N S | A | |
| 19 | 369 | Delete blank line | Formatting consistency. | N S | N | |
| 20 | 392, 396, 398, 401, 403 | Consider deleting “logical.” It’s a given that an element can be logical or physical depending on the implementation. Not used in prior clause for IMS elements. | Simplification. | N S | I | |
| 21 | 402 | Add: “(Any element that accesses the key store (i.e., STI-AS) should also be highly secure.)” | Clarification indicating the need for highly-secure key store access. | N S | A | |
| 22 | 415 (414) | “5.3.2 Reference Architecture for SIP RPH and Priority Header Signing Associated with Callback Calls” → “5.3.2 Callback Calls” | Simplification | N S | A | |
| 23 | 438 (437) | Is this paragraph the case where the Transit Function is not configured? | Provide clarification. | N S | A M | addition of: “...rather than having the transit function interact with the STI-AS using SIP.” To line 441 |
| 24 | 455 (454) | “5.4 SIP RPH Signing Call Flows for Emergency Calling” → “5.4 Call Flows” | Simplification | N S | A | |
| 25 | 456 (455) | “5.4.1 SIP RPH Signing Call Flow for Emergency (9-1-1) Originations” → “5.4.1 Emergency (9-1-1) Originations | Simplification. | N S | A | |
| 26 | 473-483 | Use sub-bullets as indicated. | Improved readability. | N S | A | |

ATIS Letter Ballot Comment Submittal Form and Consideration Report

| | | | | | | |
|----|----------------------|--|--|--------|--------|---|
| 27 | 529 (528) | Delete blank line. | Formatting consistency. | N S | N | |
| 28 | 544 (543) | “5.4.2 SIP RPH and Priority Header Signing Call Flow for Callback Calls” → “5.4.2 Callback Calls” | Simplification. | N S | A | |
| 29 | 550-551 (549-550) | “1. The PSAP Call Handling Function initiates a callback call with the callback URI from the original emergency call in the To header...” → “1. The PSAP Call Handling Function initiates a callback call with the callback URI derived from the original emergency call To header...” | Improved readability <u>readability</u> y. | N S | N | Misinterpretation of sentence by the commenter. |
| 30 | 563 (560) | Delete blank line. | Formatting consistency. | N S | N | |
| 31 | 571-572 (568-569) | “7. The Transit Function routes the SIP INVITE (with the Identity headers) over the NNI using standard inter-domain routing resolution to the egress IBCF.” → “The Transit Function routes the SIP INVITE (with the Identity headers) to the exit IBCF using standard inter-domain routing resolution. | Improved accuracy and readability. | N S | A | |
| 32 | 583 (579) | Delete blank line. | Formatting consistency. | N S | N | |
| 33 | 594-595 (589-590) | “the STI-VS includes an appropriate indicator (not defined in this document)...” → “the STI-VS includes an appropriate indicator of the verification result (defined in [Ref 2])...” | Added reference. Improved readability. | N S | A M | deletion as indicated. |
| 34 | 605 (600) | “14. The IBCF continues to set up the callback call to the CSCF.” → “The | Suggestion for providing additional detail. | N S | N | Superseded per Ericsson comments/changes |

ATIS Letter Ballot Comment Submittal Form and Consideration Report

| | | | | | | |
|----|---------------------|--|---|--------|--------|---|
| | | IBCF receives the response from the STI-VS, decides what to do based on local policy, sets the verstat in the SIP message, etc. and forwards the SIP INVITE.” | | | | |
| 35 | 606 (601) | “15. The CSCF continues to set up the callback call toward the emergency caller.” → “The CSCF strips the RPH header and forwards the SIP INVITE to the emergency caller.” | Suggestion for providing additional detail. | N S | N | |
| 36 | 630 + (625 +) | “assuming the Ms reference point.” → “via the Ms reference point” | Clearer wording. | N S | N | |
| 37 | 643 + (638 +) | “entry point IBCF” vs. “entry IBCF” | Need consistent terminology throughout? | N S | A | |
| 38 | 644 (639) | “and once the message is validated,” | Clarify how it validates the message, since Caller ID and RPH have not yet been signed. | N S | A | |
| 39 | 657 (652) | “this parameter” → “the “verstatValue” parameter” | Clarification. | N S | A | superseded by Ericsson comments/changes |
| 40 | 660 (655) | “based on the associated verstatValue returned” → “based on the associated “verstatValue” parameter returned” | Clearer wording. | N S | A | |
| 41 | 676 (670) | “The exit point IBCF must remove the ‘verstat’ from the From header...” → The exit point IBCF must remove the ‘verstat’, if any, from the From header | Clarification. | N S | A | |
| 42 | 726 – 731 (720-725) | “ Assuming the Ms reference point, upon receiving an HTTP verificationRequest 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 (for emergency originations) via the Ms reference point. | Improved readability. | N S | A M | edited per lefthand column. |

ATIS Letter Ballot Comment Submittal Form and Consideration Report

| | | | | | | |
|----|----------------------|---|-----------------------|--------|---|------------------------------|
| | | <p><u>Associated with a callback call, the STI-VS will receive a verificationRequest in one of two ways: or by receiving an HTTP verificationRequest <u>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 (for callback calls).</u> ¶The STI-VS retrieves the certificate referenced by the "x5u" field in the PASSporT protected header from the STI-CR. → "The STI-VS can receive a verification request in one of two ways: by receiving an HTTP verificationRequest associated with an emergency (9-1-1) origination via the Ms reference point from an entry IBCF in the IMS NG9-1-1 Emergency Services Network (for emergency originations), or receipt an HTTP verificationRequest or by receiving a SIP INVITE from 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, and follows the basic certificate path..."</u></p> | | | | |
| 43 | 736-737 (728-729) | "The verifier shall also follow the IETF RFC 8224-defined [Ref 13] verification procedures" → "The verifier shall also follow the verification procedures defined in IETF RFC 8224 [Ref 13]" | Improved readability. | N S | A | |
| 44 | 753-754 (744-745) | Add reference at end of sentence? | Clarification. | N S | N | Rejected due to prior edits. |

ATIS Letter Ballot Comment Submittal Form and Consideration Report

| | | | | | | |
|----|----------------------|---|---|---|---|--|
| 45 | 754-755 (745-746) | “The P-CSCF may also populate a value of “esnet.1” in the RPH.” | If the P-CSCF is doing the signing for emergency calls, should this be a "shall"? | S | N | |
|----|----------------------|---|---|---|---|--|

Other Information (e.g., Tables, Figures):

Session Initiation Protocol (SIP) Resource-Priority Header (RPH) and Priority Header 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 [Ref 16], with the extensions defined in draft-ietf-stir-rph-emergency-services-07, *Assertion Values for a Resource Priority Header Claim and a SIP Priority Header Claim 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

| | | |
|-------|--|----|
| 1 | Scope & Purpose | 1 |
| 1.1 | Scope | 1 |
| 1.2 | Purpose | 2 |
| 2 | Normative References | 2 |
| 3 | Definitions, Acronyms, & Abbreviations | 3 |
| 3.1 | Definitions..... | 3 |
| 3.2 | Acronyms & Abbreviations | 3 |
| 4 | Assumptions..... | 4 |
| 4.1 | General Assumptions..... | 5 |
| 4.2 | Architectural Assumptions..... | 5 |
| 5 | SIP RPH and Priority Header Authentication for 9-1-1 | 6 |
| 5.1 | Protocol Support | 7 |
| 5.1.1 | <i>RFC 8225: PASSporT: Personal Assertion Token</i> | 7 |
| 5.1.2 | <i>RFC 8224: Authenticated Identity Management in the Session Initiation Protocol (SIP)</i> | 7 |
| 5.1.3 | <i>RFC 8443: Personal Assertion Token (PASSporT) Extension for Resource Priority Authorization</i> | 8 |
| 5.1.4 | <i>Assertion Values</i> | 8 |
| 5.2 | Governance Model and Certificate Management | 9 |
| 5.3 | Reference Architecture | 9 |
| 5.3.1 | <i>Emergency (9-1-1) Originations</i> | 9 |
| 5.3.2 | <i>Callback Calls</i> | 11 |
| 5.4 | Call Flows..... | 12 |
| 5.4.1 | <i>Emergency (9-1-1) Originations</i> | 12 |
| 5.4.2 | <i>Callback Calls</i> | 14 |
| 6 | Procedures for SIP RPH and Priority Header Authentication | 15 |
| 6.1 | Procedures at the IBCF..... | 15 |
| 6.1.1 | <i>Entry IBCF</i> | 15 |
| 6.1.2 | <i>Exit IBCF</i> | 16 |
| 6.2 | Procedures at the STI-AS | 17 |
| 6.3 | Procedures at the STI-VS | 17 |
| 6.4 | Procedures at the P-CSCF | 18 |
| 6.5 | Procedures at the Transit Function | 18 |

Table of Figures

| | | |
|-------------|---|----|
| Figure 5-1: | Architecture for Signing SIP RPH of Emergency Originations..... | 9 |
| Figure 5-2: | Architecture for Signing SIP RPH of Callback Calls | 11 |
| Figure 5-3: | Emergency Origination SIP RPH Signing Call Flow | 12 |
| Figure 5-4: | Callback Call SIP RPH Signing Call Flow..... | 14 |

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, *PASSporT Extension for Resource-Priority Authorization*, with the assertion values described in draft-ietf-stir-rph-emergency-services-07, *Assertion Values for a Resource Priority Header Claim and a SIP Priority Header Claim in Support of Emergency Services Networks*, 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 draft-ietf-stir-rph-emergency-services-07 [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.

44 The scope of this ATIS standard is limited to the cryptographic signing and verifying of SIP RPH and Priority header
45 field contents associated with emergency and callback calls (i.e., RPH values in the "esnet" namespace and a
46 Priority header value of "psap-callback"). This standard does not address caller identity (SHAKEN) authentication
47 and verification associated with emergency calls and callback calls, except in the context of call flow descriptions,
48 nor does it discuss specific impacts to call processing or routing procedures associated with the use of the Priority
49 header to mark callback calls. Finally, the display of information associated with the verification of SIP RPH and
50 Priority header values is outside the scope of this document.

51

52 1.2 Purpose

53 Illegitimate spoofing of SIP RPH values in the "esnet" namespace in the signaling associated with emergency calls
54 and callback calls is a concern for Public Safety. NG9-1-1 System Service Providers will interconnect with multiple
55 Originating Service Providers and will benefit from knowing whether the SIP RPH value received in incoming
56 signaling can be trusted. Likewise, home network providers serving emergency callers will benefit from knowing
57 whether the Priority header accompanying a callback call can be trusted before applying special processing or
58 routing to such calls. The purpose of this standard is to provide a framework for cryptographically signing the SIP
59 RPH and Priority header fields and verifying that the SIP RPH and Priority header fields can be trusted to mitigate
60 against unauthorized spoofing of, or tampering with, the information conveyed in the SIP RPH or Priority header.
61 This framework will leverage the SHAKEN infrastructure for caller identity authentication and verification and will
62 describe how the PASSporT "rph" extension defined in IETF RFC 8443 [Ref 16], with the RPH assertion values and
63 SIP Priority header claim described in draft-ietf-stir-rph-emergency-services-07 [Ref 7], can be used for the purpose
64 of providing a trust mechanism for the SIP RPH associated with emergency calls and the SIP RPH and Priority
65 header associated with callback calls that cross IP NNI boundaries.

66

67 2 Normative References

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

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

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

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

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

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

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

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

83 [Ref 7] draft-ietf-stir-rph-emergency-services-07, *Assertion Values for a Resource Priority Header Claim and a SIP*
84 *Priority Header Claim in Support of Emergency Services Networks.*³

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

- 86 [Ref 9] IETF RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL)*
 87 *Profile*.³
- 88 [Ref 10] IETF RFC 7090, *Public Safety Answering Point (PSAP) Callback*.³
- 89 [Ref 11] IETF RFC 7135, *Registering a SIP Resource Priority Header Field Namespace for Local Emergency*
 90 *Communications*.³
- 91 [Ref 12] IETF RFC 7230, *Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing*.³
- 92 [Ref 13] IETF RFC 8224, *Authenticated Identity Management in the Session Initiation Protocol*.³
- 93 [Ref 14] IETF RFC 8225, *PASSporT: Personal Assertion Token*.³
- 94 [Ref 15] IETF RFC 8226, *Secure Telephone Identity Credentials: Certificates*.³
- 95 [Ref 16] IETF RFC 8443, *PASSporT Extension for Resource-Priority Authorization*.³
- 96

97 **3 Definitions, Acronyms, & Abbreviations**

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

100

101 **3.1 Definitions**

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

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

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

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

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

117

118 **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 |
| LRP | 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 |

119

120

121

4 Assumptions

122 4.1 General Assumptions

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

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

152

153 4.2 Architectural Assumptions

154 In keeping with the SHAKEN reference architecture described in ATIS-1000074-E [Ref 5], which shows a Call
155 Session Control Function (CSCF) interacting with a Secure Telephone Identity Authentication Service (STI-AS) (in
156 the originating network) and a Secure Telephone Identity Verification Service (STI-VS) (in the terminating network),
157 initial discussions related to the architecture to support the application of SHAKEN to 9-1-1 assumed that, for 9-1-1
158 originations, the Emergency Call Session Control Function (E-CSCF) in the originating IMS network would interact
159 with the STI-AS, and an E-CSCF (in an IMS-based NG9-1-1 Emergency Services Network) or an i3 Emergency
160 Service Routing Proxy (ESRP) (in an i3 NG9-1-1 Emergency Services Network) would interact with the STI-VS.
161 However, there is currently no reference point defined in 3GPP standards that supports interactions between an E-
162 CSCF and an Application Server. 3GPP TS 23.228, *3rd Generation Partnership Project; Technical Specification
163 Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2.3*, and 3GPP TS 24.229 [Ref 2] do,
164 however, describe the use of the Ms reference point between an IBCF and an Application Server over which HTTP
165 1.1, as specified in IETF RFC 7230, *Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing*, is
166 currently defined. Specifically, Annex V of 3GPP TS 24.229 [Ref 2] defines a signingRequest/signingResponse and
167 verificationRequest/verificationResponse to support caller identity signing and verification. Note that this
168 mechanism is also supported by ATIS-1000082, *Technical Report on SHAKEN APIs for a Centralized and Signature
169 Validation Server*, where the exit IBCF in the originating network is the "Authenticator" and the entry IBCF in the
170 IMS NG9-1-1 Emergency Services Network is the "Verifier".

171 Based on 3GPP TS 24.229 [Ref 2], to get an asserted identity signed, the client sends an HTTP POST request
172 towards the signing server containing a PASSporT SHAKEN object. As currently defined, the signingRequest
173 includes "orig" and "dest" claims, "iat", and "origid". The signingRequest may also include an "attest" parameter that
174 identifies the relation between the service provider attesting the identity and the subscriber. (According to 3GPP TS
175 24.229 [Ref 2], the signingRequest may also include a "div" claim identifying the diverting user, if applicable.) The

176 ability for an IBCF to include this information in a signingRequest sent to an STI-AS has other architectural
177 implications. Specifically, it suggests the need for an upstream element, such as a P-CSCF, in the case of an
178 emergency origination, to provide attestation information associated with the caller identity, and to convey the
179 attestation level in the SIP signaling (e.g., in an Attestation-Info header) sent to an exit IBCF. According to 3GPP
180 TS 24.229 [Ref 2] and ATIS-1000082 [Ref 6], upon receiving an HTTP 200 (OK) response to the signingRequest,
181 the IBCF (Authenticator) will include the signingRequest response data in an Identity header field in the forwarded
182 SIP request. This model differs from the framework architecture example described in ATIS-1000074-E [Ref 5],
183 where the SIP INVITE is forwarded by a CSCF to the STI-AS and the STI-AS is responsible for attestation, as well
184 as creating and adding an Identity header field to the request. The reference architecture described in Clause 5.3.1
185 and flow described in Clause 5.4.1 of this standard illustrate the use of the Ms reference point to support caller
186 identity, as well as RPH signing associated with emergency originations. The IBCF procedures described in Clause
187 6.1 of this standard also assume the use of the Ms reference point between the IBCF and the STI-AS/STI-VS to
188 support caller identity and RPH signing/verification.

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

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

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

213

214 **5 SIP RPH and Priority Header Authentication for 9-1-1**

215 In addition to caller identity authentication/verification, 9-1-1 calls and callback calls may also be subject to RPH
216 signing and, in the case of callback calls, SIP Priority header signing. In the context of 9-1-1 calls, a signed RPH
217 received in an incoming SIP INVITE message will convey to an NG9-1-1 Emergency Services Network provider
218 that they can trust that the RPH was populated by the Originating Service Provider, as opposed to being inserted
219 by a threat agent. In the context of callback calls, a signed RPH and SIP Priority header would indicate that the
220 NG9-1-1 Emergency Services Network provider asserts that they recognize the call is a callback call and, as such,
221 that an RPH value in the "esnet" namespace and a SIP Priority header with the value "psap-callback" are
222 appropriate. The SHAKEN model specified in ATIS-1000074-E [Ref 5] can be leveraged to cryptographically sign
223 and verify the SIP RPH field in SIP INVITE messages associated with 9-1-1 and callback calls and the SIP Priority
224 header associated with callback calls. Using the PASSporT extension defined in IETF RFC 8443 [Ref 16], the RPH
225 assertion values and SIP Priority header claim described in draft-ietf-stir-rph-emergency-services-07 [Ref 7] and
226 the associated STI protocols, SIP RPH and Priority header field contents can be signed and verified.

227 The framework specified in this standard supports a trust mechanism for SIP RPH values associated with
228 emergency calls and callback calls, and SIP Priority header values associated with callback calls, crossing IP NNI

229 boundaries. A high-level description of the RPH/SIP Priority header signing flow supported by the framework
 230 specified in this standard is as follows:

231 For emergency calls:

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

236 For callback calls:

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

242

243 **5.1 Protocol Support**

244 This ATIS standard uses the PASSporT "rph" extension specified in IETF RFC 8443 [Ref 16], the RPH assertion
 245 values described in draft-ietf-stir-rph-emergency-services-07 [Ref 7], and associated STI protocols for cryptographic
 246 signing of the SIP RPH field in support of emergency service calls. Similarly, this ATIS standard uses the PASSporT
 247 "rph" extension specified in IETF RFC 8443 [Ref 16], the RPH assertion values and SIP Priority header claim
 248 described in draft-ietf-stir-rph-emergency-services-07 [Ref 7], and associated STI protocols for cryptographic
 249 signing of the SIP RPH/Priority header fields in support of callback calls.

250

251 **5.1.1 RFC 8225: PASSporT: Personal Assertion Token**

252 IETF RFC 8225, PASSporT: *Personal Assertion Token* [Ref 14], defines a token-based signature that combines
 253 the use of JavaScript Object Notation (JSON) Web Tokens, JSON Web Signatures, and X.509 certificate key pairs,
 254 or Public Key Infrastructure, to create a trusted signature. The authorized owner of the certificate used to generate
 255 the signature can be validated and traced back to the known trust anchor who signed the certificate. The PASSporT
 256 includes a number of claims the signer of the token is asserting. The associated public certificate is used to verify
 257 the digital signature and the claims included in the PASSporT. The public certificate is also used to validate the
 258 entity that signed the token, as defined in IETF RFC 8226, *Secure Telephone Identity Credentials: Certificates* [Ref
 259 15]. The validated claims and the validated identity of the entity signing the claims can be used to determine the
 260 level of trust in the originating entity and their asserted SIP RPH information.

261

262 **5.1.2 RFC 8224: Authenticated Identity Management in the Session Initiation Protocol** 263 **(SIP)**

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

270

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.

271 5.1.3 RFC 8443: Personal Assertion Token (PASSporT) Extension for Resource Priority 272 Authorization

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

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

```
281 {
282   "typ":"passport",
283   "ppt":"rph",
284   "alg":"ES256",
285   "x5u":"https://www.example.org/cert.cer"
286 }
```

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

291

292 5.1.4 Assertion Values

293 draft-ietf-stir-rph-emergency-services-07 [Ref 7] adds new assertion values for the Resource-Priority Header ("rph")
294 claim defined in IETF RFC 8443 [Ref 16] to support Emergency Services Networks for emergency call origination
295 and callback.

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

```
298 {
299   "dest":{"uri":["urn:service:sos"]},
300   "iat":1443208345,
301   "orig":{"tn":["12155551212"]},
302   "rph":{"auth":["esnet.1"]}
303 }
304
```

305 In addition, draft-ietf-stir-emergency-services-07 [Ref 7] defines a new SIP Priority header claim ("sph") for
306 protection of the "psap-callback" value as part of the "rph" PASSporT extension to support the security of
307 Emergency Services Networks for emergency callbacks. The "sph" claim shall only be used for authorized
308 emergency callbacks and corresponds to a SIP Priority header field with the value "psap-callback". For emergency
309 callbacks, the "orig" claim of the "rph" PASSporT represents the PSAP telephone number. The "dest" claim contains
310 the telephone number representing the emergency caller that is being called back. The following is an example of
311 an "rph" claim for a SIP Resource-Priority Header field with an "esnet.0" assertion and an "sph" claim:

```
312 {
313   "dest":{"tn":["12155551212"]},
314   "iat":1443208345,
315   "orig":{"tn":["12155551213"]},
316   "rph":{"auth":["esnet.0"]}
317   "sph":"psap-callback"
```

318 }
 319

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

322

323 **5.2 Governance Model and Certificate Management**

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

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

330

331 **5.3 Reference Architecture**

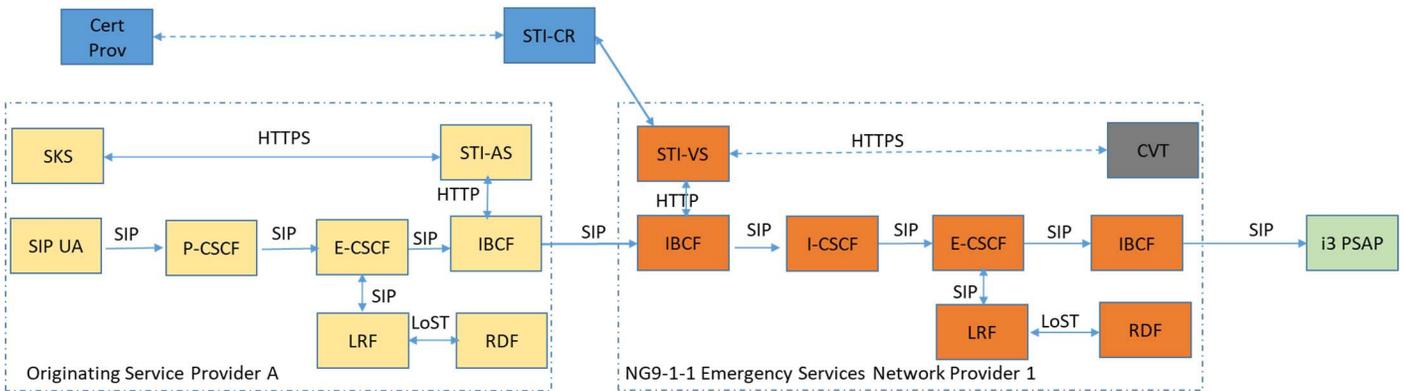
332 **5.3.1 Emergency (9-1-1) Originations**

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

341 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
 342 an Identity header field or to request verification of a signed identity in an Identity header field. The currently defined
 343 protocol to be used on the Ms Reference Point is HTTP 1.1, as specified in IETF RFC 7230 [Ref 12].

344

345



346

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

348

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

350 **IMS Elements:**

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

- 353
- 354
- 355
- 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.
- 356
- 357
- 358
- 359
- NOTE: As specified in 3GPP TS 24.229 [Ref 2] and ATIS-0700015, *ATIS Standard for Implementation of 3GPP Common IMS Emergency Procedures for IMS Origination and ESI/Net/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.
- 360
- 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.
- 361
- 362
- 363
- 364
- 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.
- 365
- 366
- 367
- 368
- 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.

369

370 SHAKEN Elements

- 381
- 382
- 383
- 384
- 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.

385

386 Public Safety Elements

- 387
- 388
- 389
- 390
- 391
- 392
- 393
- 394
- 395
- 396
- 397
- 398
- 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.

399

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).

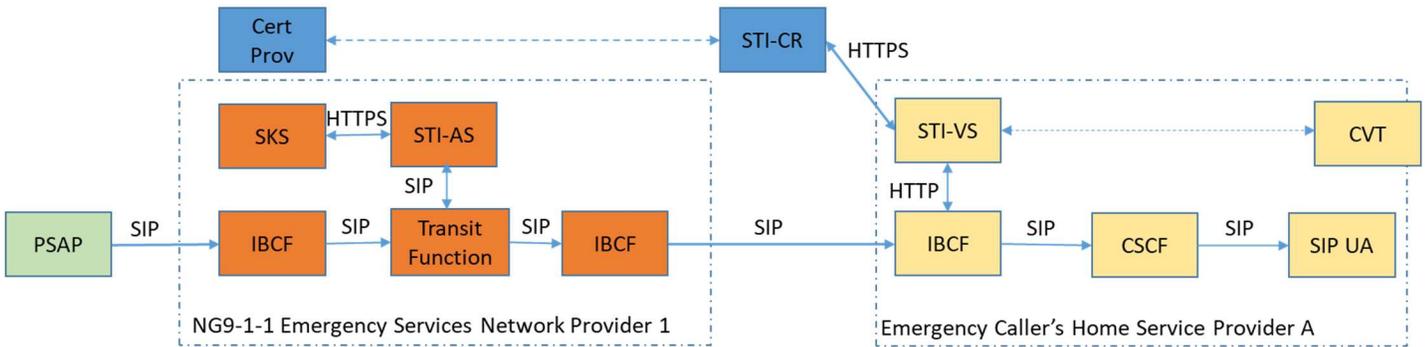


Figure 5-2: Architecture for Signing SIP RPH of Callback Calls

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

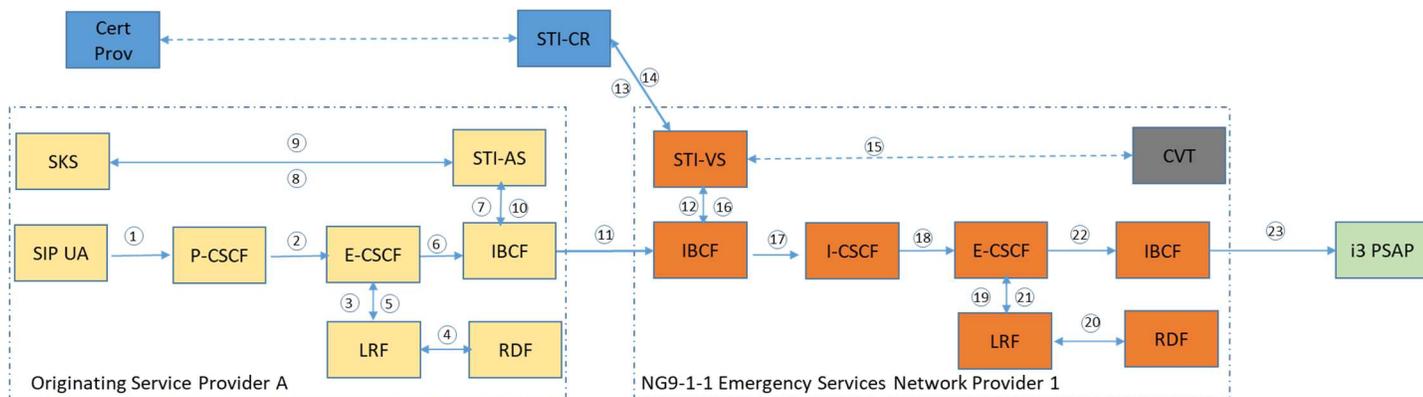
- Transit Function – As described in 3GPP TS 23.228 [Ref 1], a Transit Function is an element that determines where to route a session based on an analysis of the destination address. This includes routing to destinations in other IMS networks or the PSTN. In the context of the emergency calling, the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

446 **5.4 Call Flows**

447 **5.4.1 Emergency (9-1-1) Originations**

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

449



450

451

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

452

453

454

455

456

457

458

459

460

461

462

463

464

465

466

467

468

469

470

471

472

473

474

475

476

477

478

479

480

481

482

483

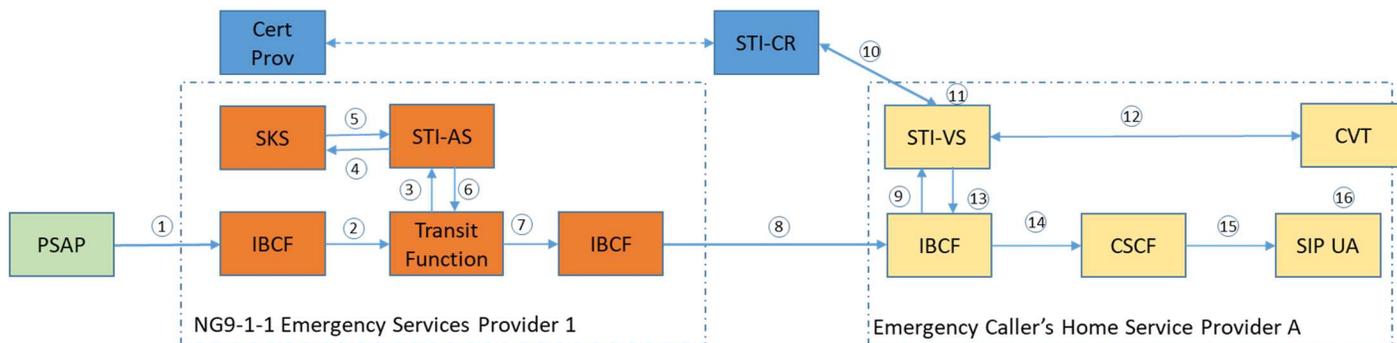
1. The originating SIP UA, which first registers and is authenticated to the P-CSCF, creates a SIP INVITE with a telephone number identity.
 2. The P-CSCF in the originating network adds a P-Asserted-Identity header field asserting the caller identity of the originating SIP UA, and an RPH with value "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].

- 484
485
486
487
488
489
490
491
492
493
494
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' 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.
- 495
496
497
498
499
500
501
502
503
504
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).
- 505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
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.

534 23. The (exit) IBCF forwards the SIP INVITE to the i3 PSAP with the appropriate "verstat" value in the P-
 535 Asserted-Identity header, the Priority-Verstat header field and the Identity headers, and normal call
 536 processing associated with the emergency origination continues.⁵
 537

5.4.2 Callback Calls

539 This call flow description is based on the reference architecture illustrated in Figure 5-2.
 540



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

- 542
- 543 1. The PSAP Call Handling Function initiates a callback call with the callback URI from the original
 544 emergency call in the To header and Request-URI, the TN of the PSAP originating the callback (i.e.,
 545 sip:TN@<psapdomain>;user=phone) in the From and P-Asserted-Identity headers, "psap-callback" in
 546 the Priority header, and "esnet.0" in the Resource-Priority Header.
 547
 - 548 2. Upon receiving the SIP INVITE from the PSAP, the entry IBCF applies general screening rules to the
 549 request and, based on local policy, adds an Origination-Id header, to indicate from where the request
 550 was received, and an Attestation-Info header to the SIP INVITE. It then forwards the SIP INVITE to the
 551 Transit Function.
 - 552 3. The Transit Function uses the destination address (i.e., the callback URI) in the Request-URI to
 553 determine the routing for the call. Before forwarding the call to the interconnecting network, the Transit
 554 Function sends the request to the STI-AS for authentication and signing of the caller identity and signing
 555 of the RPH and Priority header.
 556 NOTE: The STI-AS must be invoked after originating call processing (i.e., after the Transit Function determines
 557 that the interconnected network over which the call will be routed is an IP network).
 558
 - 559 4. The STI-AS determines, through service provider-specific means, the legitimacy of the content of the
 560 caller identity and the RPH and SIP Priority header fields. The STI-AS then securely requests its private
 561 key from the SKS.
 - 562 5. The SKS provides the private key in the response, and the STI-AS signs and adds Identity header fields
 563 per IETF RFC 8224 [Ref 13].
 - 564 6. The STI-AS returns the SIP INVITE which includes a signed Identity header field value for the caller
 565 identity and signed Identity header field values for the RPH and SIP Priority header in JSON objects.
 - 566 7. The Transit Function routes the SIP INVITE (with the Identity headers) to the exit IBCF using standard
 567 inter-domain routing resolution. If, based on local policy, a "verstat" is present in the SIP INVITE
 568 received by the Transit Function, the IBCF shall remove the "verstat" before forwarding the call to the
 569 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.

- 570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
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.
 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.

603 **6 Procedures for SIP RPH and Priority Header Authentication**

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

606

607 **6.1 Procedures at the IBCF**

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

615

616 **6.1.1 Entry IBCF**

617 For emergency (9-1-1) originations, the entry IBCF associated with the NG9-1-1 Emergency Services Network will
618 perform normal border control functions. As described in clause 5.10.10.2 of 3GPP TS 24.229 [Ref 2], when
619 receiving an initial SIP INVITE containing one or more SIP Identity header fields, the IBCF shall determine the caller
620 identity to be verified by decoding the Identity header field containing a PASSporT SHAKEN JSON Web Token.
621 The IBCF shall also determine the RPH value to be verified by decoding the Identity header associated with the

622 signed RPH. The IBCF shall then build and send a verificationRequest to the STI-VS, assuming the Ms reference
623 point. Upon receiving a verificationResponse with a "verstatValue" parameter reflecting the verification status of the
624 Identity header associated with calling identity, the IBCF shall add this parameter to the verified identity in the SIP
625 From header field or the SIP P-Asserted-Identity header field in the forwarded SIP request. If a "verstat" parameter
626 is already present in the From or P-Asserted-Identity header of the received SIP INVITE, the entry IBCF shall
627 remove it. The entry IBCF shall also populate a Priority-Verstat header field in the outgoing SIP INVITE, based on
628 the associated "verstatPriority" parameter returned in the verificationResponse, to convey the verification status of
629 the Identity header associated with the RPH.

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

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

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

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

654

655 **6.1.2 Exit IBCF**

656 For an emergency (9-1-1) origination, the exit IBCF in the Originating Service Provider network can interact with an
657 STI-AS via the Ms reference point for the signing of caller identity and RPH information, if available in an incoming
658 request. Specifically, the exit IBCF sends an HTTP POST containing two signing requests over the Ms reference
659 point to the STI-AS. The signingRequest associated with the caller identity will include an "attest" parameter that
660 contains the attestation information and an "origid" populated based on local policy or received by the IBCF in
661 Attestation-Info and Origination-Id headers, respectively, as well as other PASSporT information (i.e., "orig", "dest",
662 and "iat"). The signingRequest associated with the RPH shall include an "rph" claim as described in IETF RFC 8443
663 [Ref 16] that contains an "auth" key and assertion value of "esnet.1", as described in draft-ietf-stir-rph-emergency-
664 services-07 [Ref 7], along with the "orig", "dest", and "iat". The exit IBCF shall populate the assertion value in the
665 signingRequest based on the RPH field in the received SIP INVITE. The exit IBCF includes the signed Identity
666 headers received in the HTTP signing responses in the outgoing request. The exit IBCF shall remove the 'verstat',
667 if any, from the From header or P-Asserted-Identity header prior to sending the SIP INVITE over the IP NNI to the
668 Emergency Services Network. As described in Clause 5.4.1, the Originating Service Provider may, as an
669 implementation option, determine what other information related to caller identity and RPH authentication will be
670 forwarded to the interconnected network, based on the capabilities of the target Emergency Services Network.

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

674 For callback calls, if the NG9-1-1 Emergency Services Network supports caller identity authentication and RPH and
675 SIP Priority header signing, the exit IBCF may, based on local policy, be responsible for interacting with an STI-AS.

676 If so, the exit IBCF will send an HTTP POST containing two signing requests, assuming the Ms reference point to
677 the STI-AS. The signingRequest associated with the caller identity will include an "attest" parameter that contains
678 the attestation information and an "origid" populated based on local policy or received by the IBCF in Attestation-
679 Info and Origination-Id headers, respectively, as well as other PASSporT information (i.e., "orig", "dest", and "iat").
680 The signingRequest associated with the RPH/Priority header will include an "rph" claim that contains an "auth" key
681 and assertion value of "esnet.0" and a "sph" claim set to "psap-callback", as described in draft-ietf-stir-rph-
682 emergency-services-07 [Ref 7], along with an "orig", "dest", and "iat". The exit IBCF shall use the identityHeader
683 parameters received in the signing responses from the STI-AS to populate Identity headers in the outgoing SIP
684 INVITE associated with the callback call.

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

688

689 **6.2 Procedures at the STI-AS**

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

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

709

710 **6.3 Procedures at the STI-VS**

711 The STI-VS is an application server that performs the function of the verification service defined in IETF RFC 8224
712 [Ref 13]. In the context of emergency calling, the STI-VS provides verification services applicable to emergency
713 calls destined for PSAPs that are served by an NG9-1-1 Emergency Services Network and callback calls destined
714 for the emergency caller. Associated with an emergency (9-1-1) origination, the STI-VS will receive an HTTP
715 verificationRequest from an entry IBCF in the IMS NG9-1-1 Emergency Services Network via the Ms reference
716 point. Associated with a callback call, the STI-VS will receive a verificationRequest in one of two ways: by receiving
717 an HTTP verificationRequest over an Ms reference point from an IBCF in the emergency caller's home network, or
718 by receiving a SIP INVITE from a CSCF in the emergency caller's home network. The STI-VS retrieves the
719 certificate referenced by the "x5u" field in the PASSporT protected header from the STI-CR, and follows the basic
720 certificate path processing as described in IETF RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and*
721 *Certificate Revocation List (CRL) Profile*, following the chain until the root is reached. The STI-VS ensures that the
722 root certificate is on the list of trusted Secure Telephone Identity Certification Authorities (STI-CAs). The STI-VS
723 validates that the PASSporT information provided in the Identity headers contained in the verificationRequest
724 includes the SHAKEN claims and "rph" claim. The verifier shall also follow the verification procedures defined in
725 IETF RFC 8224 [Ref 13] to check the corresponding date, origination and destination identities, with the restrictions
726 specified in ATIS-1000074-E [Ref 5]. If an Ms reference point is used to interact with the ST-VS, the STI-VS will
727 return a "verstatValue" parameter (associated with the "identityHeader" parameter in the verificationRequest) and
728 a "verstatPriority" parameter (associated with the "rph" claim in the "identityHeaders" parameter in the
729 verificationRequest) in an HTTP verificationResponse. If a SIP interface is used to interact with the STI-VS, the STI-

730 VS will return a "verstat" parameter in the P-Asserted-Identity or From header, and a Priority-Verstat header field in
731 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
732 may include another appropriate indicator (not defined in this document) in the verificationResponse based on
733 interactions with the CVT. The STI-VS must be invoked prior to terminating call processing associated with the
734 emergency call (e.g., before routing URI is determined).

735

736 **6.4 Procedures at the P-CSCF**

737 A P-CSCF operating in an Originating Service Provider network that supports caller identity authentication and RPH
738 signing may, based on local policy, be responsible for inserting attestation information related to the asserted caller
739 identity and populating the RPH in a SIP INVITE associated with an emergency origination. According to 3GPP TS
740 24.229 [Ref 2], when a node performs attestation of an identity in an incoming request or can attest to the origin of
741 the request, the node can inform a downstream node about what kind of attestation the node has performed. Based
742 on local policy, if the P-CSCF is responsible for providing attestation information associated with the caller identity
743 for an authenticated emergency call, the P-CSCF will insert a "verstat" parameter in the P-Asserted-Identity header,
744 an optional Attestation-Info header field in the SIP INVITE with a value of "A", "B" or "C", as defined in ATIS-
745 1000074-E [Ref 5], associated with the caller identity, and an optional origination identifier in an Origination-Id
746 header field. The P-CSCF may also populate a value of "esnet.1" in the RPH.

747

748 **6.5 Procedures at the Transit Function**

749 The Transit Function is expected to adhere to the procedures described in Clauses 4.15.3 and 5.19 of 3GPP TS
750 23.228 [Ref 1] with the following clarifications.

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