ATIS-1000078

National Security / Emergency Preparedness Priority Service Session Initiation Protocol Resource-Priority Header (SIP RPH) Signing and Verification using PASSporTs

JOINT STANDARD

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

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

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

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

ATIS-1000078, National Security / Emergency Preparedness Priority Service Session Initiation Protocol Resource-Priority Header (SIP RPH) Signing and Verification using PASSporTs

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

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

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

ATIS-1000078

ATIS Standard on

National Security / Emergency Preparedness Priority Service Session Initiation Protocol Resource-Priority Header (SIP RPH) Signing and Verification using PASSporTs

Alliance for Telecommunications Industry Solutions

Approved September 13, 2021

Abstract

This standard defines how the extension to the IETF Personal Assertion Token (PASSporT) [IETF RFC 8443, *PASSporT Extension for Resource-Priority Authorization*] and the associated Secure Telephone Identity Revisited (STIR) mechanisms are used to sign the Session Initiation Protocol Resource-Priority Header (SIP RPH) field of National Security / Emergency Preparedness (NS/EP) Priority Services calls (i.e., calls containing the “ets” and/or “wps” namespace parameter values) and convey assertions of authorization for Resource-Priority. Specifically, this standard provides a mechanism for an originating service provider to cryptographically sign the SIP RPH field of an authorized NS/EP Priority Service call and allow a receiving service provider to verify the validity of the authorization for Resource-Priority and act on the information with confidence (i.e., verifying that the RPH information has not been spoofed or compromised).

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.

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 a optional capability that could augment the standard. The standard is fully functional without the incorporation of this optional capability.

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

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

Table of Contents

Table of Figures

ATIS Standard on –

National Security / Emergency Preparedness Priority Service Session Initiation Protocol Resource-Priority Header (SIP RPH) Signing and Verification using PASSporTs

1 Scope & Purpose

1.1 Scope

IETF RFC 4412, *Communications Resource Priority for the Session Initiation Protocol (SIP)* [Ref 4], specifies use of the Session Initiation Protocol 'Resource-Priority' Header (SIP RPH) field for communicating Resource-Priority. As specified in IETF RFC 4412 [Ref 4], the SIP RPH field may be used by SIP user agents, including Public Switched Telephone Network (PSTN) gateways and terminals, and SIP proxy servers to influence prioritization afforded to communications sessions, including PSTN calls.

The SIP RPH “ets” and “wps” namespace parameters are defined and used to support National Security / Emergency Preparedness (NS/EP) Priority Service calls which include Wireless Priority Service (WPS), Government Emergency Telecommunication Service (GETS) and Next Generation Network Priority Services (NGN-PS) calls in IP-based networks. However, the SIP RPH field could be spoofed and abused by unauthorized entities impacting NS/EP Priority Service communications. For example, NS/EP Service Providers receiving SIP RPHs across IP Network-to-Network Interconnections (IPNNIs) have difficulty determining whether the SIP RPH was populated by an authorized NS/EP Service Provider, or whether it was spoofed or inserted by an unauthorized entity.

This ATIS standard describes a framework leveraging the Signature-based Handling of Asserted information using toKENs (SHAKEN) framework specified in ATIS-1000074, *Signature-based Handling of Asserted information using toKENs (SHAKEN)* [Ref 2], to cryptographically sign and verify the SIP RPH field of NS/EP Priority Service calls using the “rph” Personal Assertion Token (PASSporT) extension defined in IETF RFC 8443 [Ref 8] and the associated Secure Telephone Identity (STI) protocols. There are some cross relationships between Caller ID signing and verification using a “shaken” PASSporT and SIP RPH signing and verification using the “rph” PASSporT extension defined in IETF RFC 8443 [Ref 8]. However, Caller ID signing and verification using SHAKEN is not an NS/EP Priority Service requirement per se; it is only discussed in this standard to highlight cross relationships.

This ATIS standard is intended to provide a framework and guidance on how to use the “rph” PASSporT extension defined in IETF RFC 8443 [Ref 8] and the associated STI protocols to cryptographically sign and verify the SIP RPH field in support of a trust mechanism for NS/EP Priority Service calls crossing IPNNI boundaries.

The scope of this ATIS standard is limited to cryptographic signing and verification of the SIP RPH field of NS/EP Priority Service calls with the “ets” and “wps” namespace parameters, using the “rph” PASSporT extension defined in IETF RFC 8443 [Ref 8] and the associated STI protocols. The scope of this standard does not include cryptographic signing and verification of the attestation of the Caller ID of NS/EP Priority Service calls. The procedures to sign and verify attestations of the Caller ID in an NS/EP Priority Service call using “shaken” PASSporTs are specified in ATIS-1000074 [Ref 2].

1.2 Purpose

Illegitimate spoofing of the SIP RPH with “ets” and/or “wps” namespace parameters that are used to support NS/EP Priority Service calls is a concern for NS/EP Service Providers. NS/EP Service Providers have difficulty in determining whether a call with a SIP RPH received over IPNNIs with multiple service providers should be trusted and admitted with the SIP RPH. The purpose of this standard is to provide a framework to cryptographically sign and verify SIP RPH fields containing “ets” and/or “wps” namespace parameters that can be used as a trust mechanism to mitigate unauthorized spoofing or tampering of the SIP RPH field. The framework provided in this ATIS standard can be used in the originating network authorizing NS/EP Priority Service calls to sign a PASSporT

claim for the RPH field of a SIP INVITE before it is sent across an IPNNI boundary, and for the receiving network to verify the PASSporT claim for the RPH field to decide whether the call should be admitted with the RPH field.

1.3 General Assumptions

The following general assumptions are made in this standard:

1. SIP RPH signing is only performed by an authenticating NS/EP Service Provider (e.g., NS/EP Service Provider performing WPS and/or GETS authorization).
2. An NS/EP Service Provider can use the same certificates for signing SIP RPH with "ets" and "wps" namespace parameters as they use for signing "shaken" PASSporTs, but is not required to do so.
3. Based on local policy, an NS/EP Service Provider may choose to honor NS/EP Priority Service calls without a signed RPH or process the calls with normal priority.
    a. This might change over time taking into account the maturity of signed RPH deployments and knowledge of the adjacent carrier.
4. Transit NS/EP Service Providers may verify a signed SIP RPH, but have to transparently pass the received Identity header associated with the SIP RPH.
5. The NS/EP Service Provider receiving a signed SIP RPH verifies the signed SIP RPH and uses the results to decide whether the call should be admitted with the SIP RPH field based on local carrier policy.
6. The PASSporT extension "rph" defined in IETF RFC 8443 [Ref 8] is used to sign the entire SIP RPH header as opposed to the individual namespaces. The PASSporT object "auth" is defined to convey that the SIP RPH header information is authorized. An NS/EP Service Provider authenticating an NS/EP Service User would sign the information in the SIP RPH header using the PASSporT "rph" extension and object "auth." The PASSporT "auth" object conveys authorization for Resource-Priority by the signing NS/EP Service Provider.
7. An NS/EP Service Provider (e.g., an authorized provider of GETS and/or WPS) would sign the SIP RPH field of an authorized NS/EP Priority Service call using an "rph" PASSporT before it is sent across an IPNNI. For example, after performing a GETS Personal Identification Number (PIN) authorization or WPS authorization, assertion about the authorization for Resource-Priority is included in a PASSporT "rph" claim in a SIP Identity header.
8. Signing of the Caller ID using a "shaken" PASSporT is separate from the signing of the SIP RPH field using an "rph" PASSporT. A separate SIP Identity header is used for "rph" PASSporT claims from that used for "shaken" PASSporT claims (i.e., "shaken" claims about Caller ID).
9. What happens inside a carrier's trust domain to trigger signing and verification of "rph" PASSporT claims (i.e., with regard to use of tagging, elements responsible for creating/validating PASSporTs, etc.) is carrier-specific and outside the scope of this ATIS standard.

2 Normative References

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

[Ref 1] ATIS-1000057, *Service Requirements for Emergency Telecommunications Service (ETS) in Next Generation Networks.*[1]

[Ref 2] ATIS-1000074, *ATIS Standard on Signature-based Handling of Asserted information using toKENs (SHAKEN).*[1]

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

[Ref 3] ATIS-1000080, *ATIS Standard on Signature-based Handling of Asserted information using toKENs (SHAKEN): Governance Model and Certificate Management.*[1]

[Ref 4] IETF RFC 4412, *Communications Resource Priority for the Session Initiation Protocol (SIP).* [2]

[Ref 5] IETF RFC 8224, *Authenticated Identity Management in the Session Initiation Protocol.*[2]

[Ref 6] IETF RFC 8225, *PASSporT: Personal Assertion Token).*[2]

[Ref 7] IETF RFC 8226, *Secure Telephone Identity Credentials: Certificates.*[2]

[Ref 8] IETF RFC 8443, *Personal Assertion Token (PASSporT) Extension for Resource Priority Authorization.*[2]

[Ref 9] 3GPP TS 24.229, *IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP).*[3]

3 Definitions, Acronyms, & Abbreviations

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

3.1 Definitions

Caller ID: The originating or calling party telephone number used to identify the caller carried either in the P-Asserted Identity or From header in the SIP message [Ref 2].

Government Emergency Telecommunications Service (GETS): GETS is one facet of the USA instantiation of Emergency Telecommunication Service (ETS) using public telecommunications networks, offered by government to authorized users for NS/EP purposes. GETS is a circuit-switched form of ETS for voice (and voiceband data) using PIN authorization, in which a user can invoke the service by dialing a GETS Access Number (GETS-AN) or GETS Number Translation (GETS-NT) from most phones served by the Public Switched Telephone Network (PSTN). GETS provides priority treatment across originating, transit and terminating networks as described in ATIS-1000057, *Service Requirements for Emergency Telecommunications Service (ETS) in Next Generation Networks* [Ref 1].

NS/EP NGN Priority Services (NS/EP NGN-PS): The evolution of legacy GETS and WPS to achieve service continuity in the packet-switched Next Generation Network (NGN), and to leverage the NGN to offer new features and priority multimedia services [Ref 1].

NOTE: NS/EP NGN-PS and NS/EP NGN-GETS are used interchangeably in ATIS standards.

Wireless Priority Service (WPS): A circuit-switched form of ETS for voice (and voiceband data) using subscription-based authentication, in which a user can invoke the service by dialing a feature code from a WPS-subscribed mobile phone served by a public wireless network. WPS provides priority treatment across originating and terminating public wireless networks, including priority radio resource assignment upon call origination and termination [Ref 1].

NOTE: Use of “NS/EP Priority Service” in this standard refers to any service supported using the “ets” and/or ”wps” namespaces (e.g., GETS, WPS and NGN-PS).

[2] Available from the Internet Engineering Task Force (IETF) at: < https://www.ietf.org/ >.

[3] Available from 3rd Generation Partnership Project (3GPP) at: < https://www.3gpp.org >

3.2 Acronyms & Abbreviations

3GPP	3rd Generation Partnership Project
AS	Application Server
ATIS	Alliance for Telecommunications Industry Solutions
CISA	Cybersecurity and Infrastructure Security Agency
CSCF	Call Session Control Function
CVT	Call Validation Treatment
DHS	Department of Homeland Security
ECD	Emergency Communications Division
ETS	Emergency Telecommunication Service
FC	Feature Code
GETS	Government Emergency Telecommunications Service
GETS-AN	GETS Access Number
GETS-NT	GETS Number Translation
HTTPS	Hypertext Transfer Protocol Secure
IBCF	Interconnection Border Control Function
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPNNI	IP Network-to-Network Interconnection
JSON	JavaScript Object Notation
NCS	National Communications System
NGN	Next Generation Network
NGN-PS	Next Generation Network Priority Services
NNI	Network-to-Network Interface
NS/EP	National Security / Emergency Preparedness
NS/EP NGN-PS AS	NS/EP NGN-PS Application Server
OEC	Office of Emergency Communications
PASSporT	Personal Assertion Token

PIN	Personal Identification Number
PKI	Public Key Infrastructure
PSN	Public Switched Network
PSTN	Public Switched Telephone Network
RPH	Resource-Priority Header
RPH-AS	RPH Authentication Service
RPH-VS	RPH Verification Service
SBC-I	Session Border Controller – Interconnection
SHAKEN	Signature-based Handling of Asserted information using toKENs
SIP	Session Initiation Protocol
SKS	Secure Key Store
SPC	Service Provider Code
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
TAS	Telephony Application Server
TrGW	Transition Gateway
UA	User Agent
URI	Uniform Resource Identifier
WPS	Wireless Priority Service

4 Overview

The SHAKEN architecture, described in ATIS-1000074 [Ref 2], describes a Call Session Control Function (CSCF) interacting with a Secure Telephone Identity Authentication Service (STI-AS) (in the originating network) and a Secure Telephone Identity Verification Service (STI-VS) (in the terminating network) for attestation, signing and verification of the Caller ID of a call.

This document is an ATIS standard that describes a framework leveraging the SHAKEN model specified in ATIS-1000074 [Ref 2] to cryptographically sign and verify the SIP RPH field of NS/EP Priority Service calls with the “ets” and/or “wps” namespace parameters, using the “rph” PASSporT extension defined in IETF RFC 8443 [Ref 8].

The framework specified in this standard can be used to support a trust mechanism for the SIP RPH field of NS/EP Priority Service calls crossing IPNNI boundaries. The basic concept of the framework involves the following:

1. **Origination - Secure Telephone Identity Authentication Service (STI-AS) for RPH**: The originating NS/EP Service Provider cryptographically signs the RPH in the initial SIP INVITE request message of an authorized NS/EP Priority Service call (e.g., WPS, GETS or NGN-PS call) using the "rph" PASSporT extension defined in IETF RFC 8443 [Ref 8] and includes a SIP Identity header before it is sent across an IPNNI boundary. The originating NS/EP Service Provider may also cryptographically sign the RPH in a SIP re-INVITE when the "ets" and/or "wps" namespace parameters are included in an existing SIP dialogue for the first time for an authorized NS/EP Priority Service call. The SIP RPH signing is only performed for authorized NS/EP Priority Service calls by an authenticating NS/EP Service Provider (i.e., NS/EP Service Provider performing GETS or WPS authorization of the NS/EP Service User).
2. **Termination - Secure Telephone Identity Verification Service (STI-VS) for RPH**: The receiving terminating NS/EP Service Provider verifies the received "rph" PASSporT for the SIP RPH field in the SIP INVITE message. The result of the verification of the "rph" PASSporT is used by the terminating NS/EP Service Provider to decide whether the RPH field should be kept or stripped, based on local carrier policy.

   NOTE: A Transit NS/EP Service Provider may verify a received SIP Identity header with a "rph" PASSporT for the SIP RPH field (i.e., to determine priority treatment within its network); but has to transparently pass the received Identity header associated with the SIP RPH field.

4.1 SIP RPH Signing Protocols Overview

This ATIS standard uses the "rph" PASSporT extension specified in IETF RFC 8443 [Ref 8] and associated STIR protocols for cryptographic signing and verifying the SIP RPH field of NS/EP Priority Service calls (i.e., calls with the "ets" and/or "wps" namespace parameters).

The following provides an overview of the associated IETF STIR protocols.

4.1.1 Personal Assertion Token (PASSporT)

IETF RFC 8225, *Personal Assertion Token (PASSporT)* [Ref 6], defines a token-based signature that combines the use of JavaScript Object Notation (JSON) Web Tokens, JSON Web Signatures, and X.509 certificate key pairs, or Public Key Infrastructure (PKI), to create a trusted signature. The authorized owner of the certificate used to generate the signature can be validated and used to trace back to the known trust anchor who signed the certificate. The PASSporT includes a number of claims the signer is asserting. The associated public certificate is used to verify the digital signature and the claims included in the PASSporT. The public certificate is also used to validate the entity that signed the PASSporT through a Service Provider Code (SPC), as defined in IETF RFC 8226, *Secure Telephone Identity Credentials: Certificates* [Ref 7]. The validated claims and the validated identity of the entity signing the claims can both be used to determine the level of trust in the originating entity and their asserted SIP RPH information.

4.1.2 Authenticated Identity Management in the Session Initiation Protocol

IETF RFC 8224, *Authenticated Identity Management in the Session Initiation Protocol* [Ref 5], defines a SIP-based framework for an authentication service and verification service using the PASSporT signature in a SIP INVITE. It defines a new Identity header field that delivers the PASSporT signature and other associated parameters. The authentication service as defined according to IETF RFC 8224 [Ref 5] adds the Identity header field to the SIP INVITE generated by the originating service provider. The SIP INVITE is delivered to the destination service provider which uses the verification service to verify the signature using the information in the SIP RPH field.

4.1.3 PASSporT Extension for Resource-Priority Authorization

IETF RFC 8443 [Ref 8] defines an optional "rph" PASSporT extension and the associated STIR mechanisms to provide a function to sign the SIP RPH field. It extends the PASSporT to allow cryptographic signing and verification

of the SIP RPH field, which is used for communications resource prioritization. It also describes how the “rph” PASSporT extension is used in SIP signaling to convey assertions of authorization of the information in the SIP RPH field.

4.2 Governance Model and Certificate Management

IETF RFC 8443 [Ref 8] indicates that the credentials (e.g., authority responsible for authorizing resource-priority) used to create the signature shall have authority over the "rph" claim and indicates that there can only be one authority per claim. The authority shall use its credentials associated with the specific service supported by the SIP namespace in the claim.

The Emergency Communications Division (ECD) (formerly Office of Emergency Communications [OEC] and formerly National Communications System [NCS]) under the Cybersecurity and Infrastructure Security Agency (CISA) of the Department of Homeland Security (DHS) is the authority for NS/EP Priority Services and the claims associated with the “ets” and “wps” namespace parameters. ECD/CISA/DHS delegates “ets” and “wps” namespace signing authority to NS/EP Service Providers.

The governance model and the management of the credentials (i.e., certificates) used by NS/EP Service Providers for cryptographic signing of the SIP RPH is not within the scope of this standard.

> NOTE: NS/EP NGN-PS Service Providers can use the same certificates for signing SIP RPH as they use for SHAKEN (i.e., Caller ID signing) including the associated SHAKEN governance and certificate management defined in ATIS-1000080, *ATIS Standard on Signature-based Handling of Asserted information using toKENs (SHAKEN): Governance Model and Certificate Management* [Ref 3], but are not required to do so.

4.3 Reference Architecture for SIP RPH Signing

The SHAKEN architecture described in ATIS-1000074 [Ref 2] describes a CSCF interacting with an STI-AS (in the originating network) and an STI-VS (in the terminating network), where the STI-AS and STI-VS are SIP application servers.

Figure 4-1 below shows a reference architecture for signing and verification of the SIP RPH for calls with “ets” and “wps” namespace parameters. It is an extension to the SHAKEN architecture defined in ATIS-100074 [Ref 2] for signing and verifying the SIP RPH of NS/EP Priority Service calls across IPNNIs. In Figure 4-1, the NS/EP Priority Service call is originated from Service Provider A’s network that performs the STI-AS function, and the NS/EP Priority Service call is terminated in Service Provider B’s network, which performs the STI-VS function in accordance with the procedures defined in IETF RFC 8443 [Ref 8] for an “rph” PASSporT. In Figure 4-1, the functional elements within black rectangular boxes are IMS and SHAKEN elements as described in ATIS-1000074 [Ref 2] while the dotted red boxes are added functional elements necessary to realize the signing and verification of the SIP RPH of NS/EP Priority Service calls.

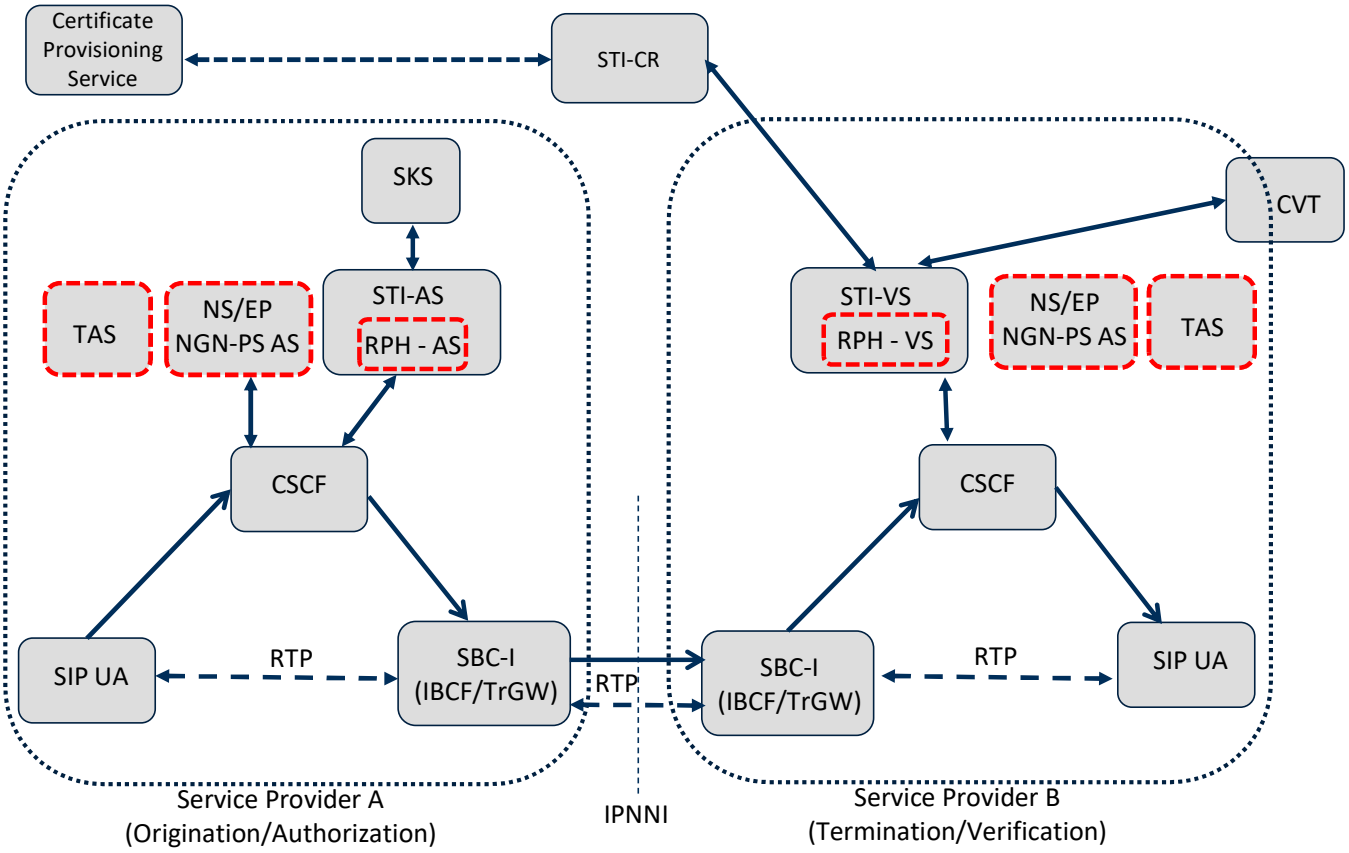

Figure 4-1 – Architecture for Signing and Verification of SIP RPH of NS/EP Calls

The reference architecture includes the following elements:

IMS Elements:

- SIP User Agent (SIP UA) – This component represents the originating and terminating end points for an NS/EP Priority Service session.
- Call Session Control Function (CSCF) – This component represents the SIP registrar and routing function. It also has a SIP application server interface.
- Session Border Controller – Interconnection (SBC-I) (Interconnection Border Control Function [IBCF] / Transition Gateway [TrGW]) – This function is at the edge of the Service Provider network and represents the IP Network-to-Network Interface (IPNNI) or peering interconnection point between service providers. It is the ingress and egress point for SIP calls between service providers.

SHAKEN Elements – Defined in ATIS-1000074 [Ref 2]

- Secure Telephone Identity Authentication Service (STI-AS)
- Secure Telephone Identity Verification Service (STI-VS)
- Call Validation Treatment (CVT)
- Secure Key Store (SKS)
- Certificate Provisioning Service
- Secure Telephone Identity Certificate Repository (STI-CR)

NS/EP Priority Service Elements

- Telephony Application Server (TAS) – This element represents telephone application processing and routing. It may include some aspects of NS/EP Priority Services call handling.
- NS/EP NGN-PS Application Server (NS/EP NGN-PS AS) – This element represents NS/EP NGN-PS processing and routing. It is the element responsible for GETS and WPS authorization.
- RPH Authentication Service (RPH-AS) – This element represents the logical authentication service for SIP RPH signing defined in IETF RFC 8443 [Ref 8].
- RPH Verification Service (RPH-VS) - This element represents the logical verification service for SIP RPH as defined in IETF RFC 8443 [Ref 8].

In keeping with the SHAKEN architecture described in ATIS-1000074[Ref 2], Figure 4-1 shows a CSCF interacting with a STI-AS (in the originating network) and a STI-VS (in the terminating network). The RPH–AS in Figure 4-1 represents logical STI-AS functions for RPH signing, and the RPH–VS represents logical STI-VS functions for verifying a signed RPH, in accordance with the procedures defined in IETF RFC 8443 [Ref 8]. The logical RPH-AS function is not responsible for performing the NS/EP Priority Service call authorization (i.e., WPS or GETS authorization). An NS/EP Priority Service call is sent to an RPH-AS function to be signed after the WPS or GETS authorization has been performed by an NS/EP NGN-PS entity (e.g., by the NS/EP NGN-PS AS or TAS). The trigger mechanism to send an NS/EP Priority Service call for signing of the SIP RPH field is based on service provider-specific implementation and out of scope of this ATIS standard.

The reference architecture in Figure 4-1 is a logical model and does not impose any restrictions on service provider implementations. Figure 4-1 shows SIP interactions between a CSCF and SIP-based Application Servers, where the Application Servers provide the logical STI-AS (RPH-AS) and STI-VS (RPH-VS) functions to sign and verify the SIP RPH field. Other approaches, not shown in Figure 4-1, are also possible such as an SBC-I (IBCF/TrGW) interacting with an AS via an Ms interface as defined in 3GPP TS 24.229, *IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocl (SDP)* [Ref 9] to sign and verify the SIP RPH field.

NOTE: 3GPP TS 24.229 [Ref 9] also defines procedures that can be used by a CSCF or IBCF for signing and verifying the SIP RPH of NS/EP Priority Service calls.

4.4 SIP RPH Signing and Verification Call Flow for NS/EP NGN-PS

Figure 4-2 below illustrates a possible SIP RPH signing and verification call flow, based on the example architecture illustrated in Figure 4-1.

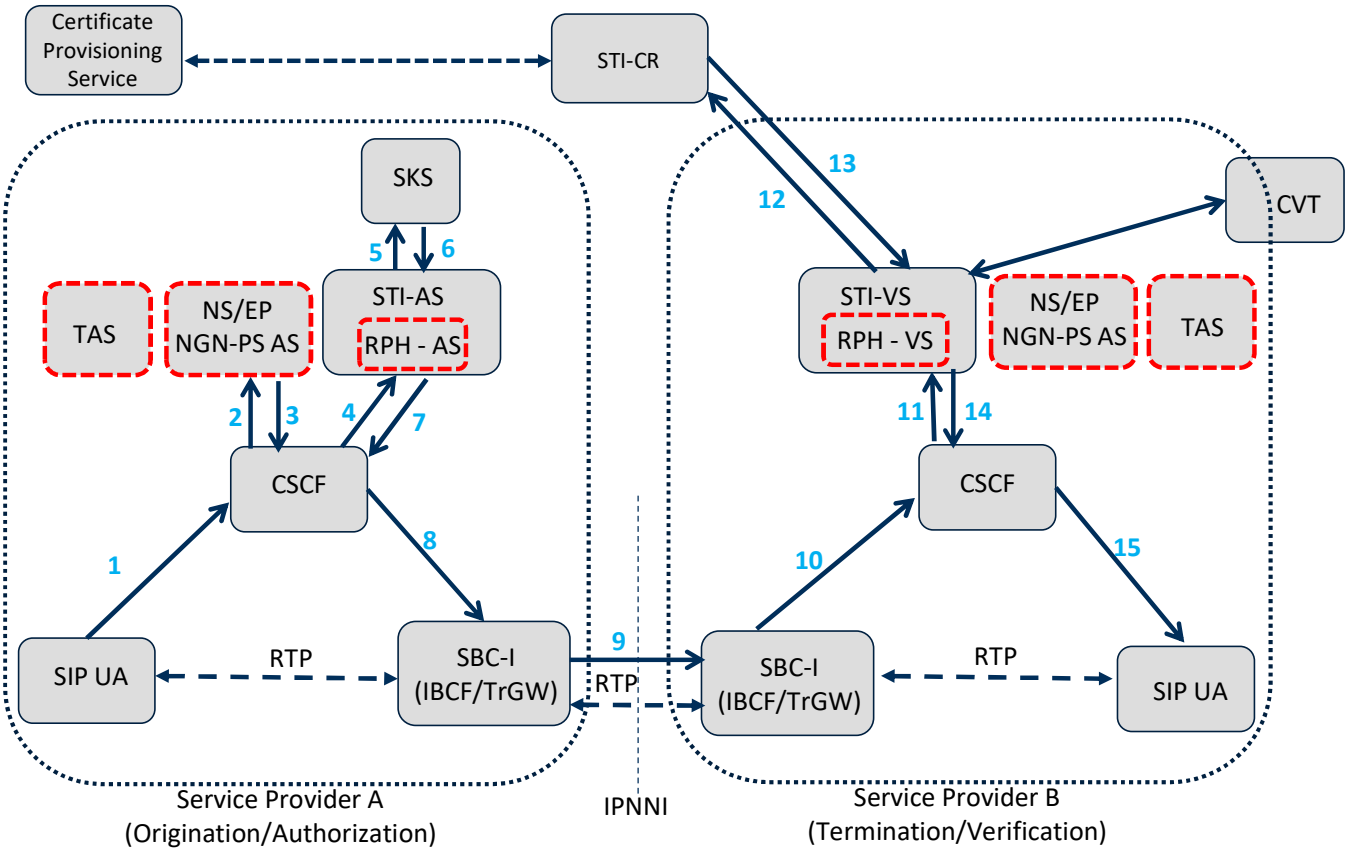

Figure 4-2 – NS/EP SIP RPH Signing and Verification Call Flow Example

1. The originating SIP UA sends a SIP INVITE for an NS/EP Priority Service call.
2. Based on the dialed digits (e.g., WPS Feature Code (FC) or GETS-AN), the originating Service Provider A routes the call to the NS/EP NGN-PS AS for priority processing and handling (e.g., WPS or GETS authorization).
3. The NS/EP NGN-PS AS appends a Resource Priority Header with “ets” and/or “wps” namespace parameters to the SIP INVITE after authorizing the NS/EP Priority Service call request.
4. The originating Service Provider A routes the SIP INVITE to the STI-AS (RPH-AS function).

   NOTE: The STI-AS is invoked after originating call processing and after the WPS or GETS authorization. The mechanism to send an NS/EP NGN-PS call to the STI-AS to sign the SIP RPH field is based on carrier-specific policy and implementation (e.g., a solution-specific mechanism for identifying calls egressing the service provider’s trusted SIP domain).

5. The RPH-AS function of the STI-AS in the originating Service Provider A network determines through service provider-specific means the legitimacy of the content of the RPH field (i.e., “ets” and “wps” namespaces) being used in the SIP INVITE. The STI-AS then securely requests its private key from the SKS.
6. The SKS provides the private key in the response, and the STI-AS signs the RPH field in the SIP INVITE per IETF RFC 8443 [Ref 8] and adds an Identity header field per IETF RFC 8224 [Ref 5].
7. The STI-AS, after signing the RPH field, passes back the SIP INVITE with the Identity header field for routing.
8. The originating Service Provider A routes the call to the egress SBC-I (IBCF/TrGW).
9. The SIP INVITE with the Identity header field is routed over the IPNNI.
10. Terminating Service Provider B's ingress SBC-I (IBCF/TrGW) receives the SIP INVITE over the IPNNI.

11. Based on the presence of the “rph” PASSporT, the terminating Service Provider B routes the SIP INVITE to the STI-VS (RPH-VS).

    NOTE: The STI-VS is invoked before admitting the call with the SIP RPH in terminating Service Provider B’s network.

12. Terminating Service Provider B's STI-VS determines the STI-CR Uniform Resource Identifier (URI) and makes an HTTPS request to the STI-CR as per ATIS-1000074 [Ref 2].
13. The STI-VS (RPH-VS) validates the certificate and then extracts the public key as per ATIS-1000074 [Ref 2]. It constructs the RFC 8224 [Ref 5] PASSporT format and uses the public key to verify the signature in the Identity header field, which validates the RPH field used for signing the SIP INVITE on the originating Service Provider STI-AS (RPH-AS).
14. The result of the STI verification is used by terminating Service Provider B to determine whether the call is to be admitted and completed with or without the RPH field. (This decision is based on local carrier policy and other policies that may be defined outside of this ATIS standard based on NS/EP Priority Service requirements). The SIP INVITE is passed back to the CSCF to set up the call to the terminating SIP UA according to NS/EP Priority Service procedures.

    NOTE: Error cases where the verification fails are discussed in Clause 5.3.2 of the SHAKEN framework, ATIS-1000074 [Ref 2].

15. The terminating SIP UA receives the SIP INVITE, and SIP processing of the call according to NS/EP Priority Service procedures continues to set up the media end-to-end.

The above call flow is intended to be illustrative and does not impose any restrictions on service provider implementations. Other approaches, not shown in Figure 4-2, are also possible such as an SBC-I (IBCF/TrGW) providing the logical STI-AS (RPH-AS) and STI-VS (RPH-VS) functions and may interact via an Ms interface (as defined in 3GPP TS 24.229 [Ref 9]) using HTTP with Application Servers to sign and verify the SIP RPH field.

5 Procedures for SIP RPH Signing

IETF RFC 8224 [Ref 5] and IETF RFC 8225 [Ref 6] define a base set of procedures for how STI fits into the SIP call flow. IETF RFC 8225 [Ref 6] defines the procedures for constructing the PASSporT. IETF RFC 8224 [Ref 5] defines an authentication service and a verification service corresponding to the STI-AS and STI-VS described in the SHAKEN reference architecture.

IETF RFC 8443 [Ref 8] defines the “rph” PASSporT extension to sign and verify claims for the SIP RPH field. This clause details the procedures required for the STI-AS (RPH-AS) function to create the required Identity header and the STI-VS (RPH-VS) function to verify the claims of the Identity header for the SIP RPH field, where the STI-AS (RPH-AS) and STI-VS (RPH-VS) are logical functions described in Clause 4.4.

5.1 PASSporT Overview

STI as defined in IETF RFC 8225 [Ref 6] specifies the use of the PASSporT. Refer to RFC 8225 [Ref 6] for the process and specific examples of a PASSporT.

5.2 PASSporT Construction and Procedures

5.2.1 PASSporT & Identity Header Construction

The PASSporT for the “rph” claim shall be constructed as defined using the base PASSporT defined in IETF RFC 8225 [Ref 6] and the “rph” PASSporT extension defined in IETF RFC 8443 [Ref 8].

The procedures defined in IETF RFC 8224 [Ref 5] shall be used to construct and include a SIP Identity header for the “rph” PASSporT in the SIP INVITE generated by the originating service provider.

5.2.2 PASSporT Extension “rph”

The standard PASSporT extension for “rph” shall be used as defined in IETF RFC 8443 [Ref 8] to sign and verify the SIP RPH field with “ets” and/or “wps” namespace parameters.

The creator of a PASSporT object adds a "ppt" value of "rph" to the header of a PASSporT object, in which case the PASSporT claims shall contain an "rph" claim, and any entities verifying the PASSporT object are required to recognize the "ppt" extension in order to process the PASSporT in question. A PASSporT header with the "ppt" included will appear as follows:

```
{
"typ":"passport",
 "ppt":"rph",
 "alg":"ES256",
 "x5u":"https://www.example.org/cert.cer"
}
```

The "rph" claim will provide an assertion of authorization, "auth" for information in the SIP RPH with “ets” and/or “wps” namespace parameter fields.

The following example from IETF RFC 8443 (Ref 8] shows an "rph" claim for a SIP RPH field with one r-value of "ets.0" and with another r-value of "wps.0" (i.e., where the ets and wps priority level of the NS/EP Service User is “0”):

```
 {
  "orig":{"tn":"12155550112"},
  "dest":{["tn":"12125550113"]},
  "iat":1443208345,
  "rph":{"auth":["ets.0", "wps.0"]}
 }
```

After the header and claims PASSporT objects have been constructed, their signature is generated normally per the guidance in IETF RFC 8225 [Ref 6] using the full form of PASSporT.

According to IETF RFC 8443 [Ref 8], the credentials (i.e., certificate) used to create the signature shall have authority over the namespace of the "rph" claim. There shall be only one authority per claim. The ECD/CISA/DHS delegates signing authority for “rph” claims with the “ets” and/or “wps” namespace parameters. As indicated in Clause 4.2, the NS/EP Service Provider can use the same credentials as those used to sign “shaken” PASSporTs, but is not required to do so.

If r-values are modified, added or dropped by intermediaries along the path, the intermediaries shall generate a new "rph" header and sign the claim with their own authority.

The use of the compact form of PASSporT is not specified in IETF RFC 8443 [Ref 8].

5.2.3 STI-AS (RPH-AS) Procedures

The STI-AS (RPH-AS) is a logical function that provides the authentication service defined in Clause 4.1 of IETF RFC 8443 [Ref 8], with the exceptions and additions specified in this clause.

After NS/EP Priority Service call processing and authorization (i.e., WPS or GETS authorization), the SIP INVITE is sent to the logical STI-AS (RPH-AS) function using a trigger mechanism based on local carrier policy and implementation (e.g., when the call is tagged as leaving the service provider's trusted SIP domain) to sign the SIP RPH field.

The STI-AS (RPH-AS) function derives the value of the "rph" claim and then securely requests its private key from the SKS.

Upon receiving the private key from the SKS, the STI-AS (RPH-AS) function signs the RPH field and returns an Identity header field value for the SIP RPH field.

5.2.4 STI-VS (RPH-VS) Procedures

The STI-VS (RPH-VS) is a logical function providing the verification service defined in Clause 4.2 of IETF RFC 8443 [Ref 8], with the exceptions and additions specified in this clause.

When a terminating NS/EP Priority Service Provider receives an NS/EP Priority Service call with an Identity header containing a "ppt" value of "rph", the SIP INVITE is sent to the logical STI-VS (RPH-VS) function using a trigger mechanism based on local carrier policy and implementation (e.g., an NS/EP Priority Service call tagged as received from outside of the carrier trusted SIP domain) to verify the signed SIP RPH. The verifier retrieves the certificate referenced in the "rph" PASSporT protected header and follows the basic certificate path processing as described in Clause 5.3.1 of ATIS-1000074 [Ref 2], following the chain until the root certificate is reached, and ensures that the root certificate is on the list of trusted STI-CAs.

The verifier validates the "rph" claim including the "iat" claim as specified in Clause 4.2 and Clause 6.2 of IETF RFC 8443 [Ref 8] respectively. The verifier shall also follow the RFC 8224 [Ref 5]-defined verification procedures to check the corresponding originating identity (i.e., the originating telephone number in the "orig" claim) and destination identity (i.e., the terminating telephone number in the "dest" claim).

If the "rph" claim is successfully validated, the RPH field is considered to be authorized and the SIP INVITE should be admitted with the RPH field and provided priority treatment according to the local carrier policy.

If the "rph" claim validation fails, the RPH field is handled as per local carrier policy. In such cases, the RPH field should be stripped and the call treated as an ordinary call.

5.2.5 Verification Error Conditions

The procedures described in Clause 5.3.2 of ATIS-1000074 [Ref 2] shall be followed.

5.2.6 Use of the Full Form of PASSporT

IETF RFC 8225 [Ref 6] supports the use of both full and compact forms of the PASSporT in the Identity header. The full form of the PASSporT shall be used in accordance with IETF RFC 8443 [Ref 8].

5.3 Other Considerations

5.3.1 Call Validation Treatment (CVT)

Post STI-VS and CVT handling of NS/EP Priority Service calls with a signed SIP RPH is specified in Clause 5.3.4 of ATIS-1000074 [Ref 2].

5.3.2 Display

Conveying the verification status of the “rph” claim to end user devices is not required for NS/EP Priority Service calls with “ets” and/or “wps” namespace parameters.

3GPP TS 24.229 [Ref 9] specifies the “Priority-Verstat” Header field with a set of values corresponding to possible “rph” PASSporT validation results. This information shall not be conveyed to the UA for NS/EP Priority Service calls.