**ATIS IPNNI Task Force**

**November 6-7, 2019**

**Reston, VA**

**Contribution**

**TITLE: NS/EP NGN-PS SIP RPH Signing Call Flow**

**SOURCE\*: Perspecta Labs, CISA ECD, AT&T, GDIT**

**ISSUE NUMBER:**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Abstract**

This contribution proposes a set of call flow scenarios for NS/EP NGN-PS SIP RPH Signing to be included in an informative Annex in Draft ATIS Standard on SIP RPH Signing using PASSPorT Tokens.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Annex A**

(normative/informative)

# A NS/EP NGN-PS SIP RPH Signing Call Flow Examples

This Annex provides illustrative example call flows for SIP RPH signing of NS/EP NGN-PS calls. It is assumed that TN signing as per [ATIS-1000074] will also occur for NS/EP NGN-PS calls, therefore, the call flow examples in this Annex consider both the TN and SIP RPH signing of NS/EP NGN-PS calls and the associated cross relationship.

The following general assumptions are made for the call flow scenarios in this Annex:

1. What happens inside a carrier’s trust domain (i.e., with regard to use of tagging, elements responsible for creating/validating tokens, etc.) is carrier-specific. Note: the call flows in Annex A are examples only, while the actual network implementations are carrier–specific.
2. The flows show the PAI field being used internally in the carrier’s network, and show PASSporT signing when the SIP INVITE leaves the network. The flows also show tagging parameters (P-headers except for PAI) are removed and replaced with PASSporT on the inter-carrier interfaces; actual network implementations are carrier–specific.
3. Each carrier’s network is different in how to determine whether the carrier is the terminating or the transit carrier. The flows presented in this report assume an I-CSCF and/or I-SBC perform a local query to the HSS to determine if the carrier is a transit or terminating carrier. This occurs before the call is sent to a PASSporT AS, to determine if the call should be sent to the PASSporT AS.
4. The flows show information in the PASSporT token being moved into a PAI field for transmission across the terminating carrier’s network. This is based on carrier-specific implementations and other approaches are possible.

## Architectural reference assumptions

### Originating Network - TN Signing and RPH Signing of NS/EP NGN-PS Calls

It is assumed that TN signing of NS/EP NGN-PS calls would occur as per [ATIS-1000074]. It is assumed that TN signing would be implemented at the edge and calls will be signed upon egress to another carrier (e.g. at the egress I-SBC) as shown in Figure A 1. In Figure A 1, the egress I-SBC uses the SHAKEN API to request Signing from a Signing service (i.e., the STI-AS), using received attestation and origid information in order to perform the authentication/signing. To provide this information to the I-SBC, it is assumed that a “tagging” function is introduced to add two new P-headers to the SIP INVITE to convey this information:

* P-Attestation-Indicator,
* P-Origination-Id, and
* verstat is also added to the INVITE.

It is assumed that the “tagging” function is performed on all call originations, since the originating TAS does not yet know how the call will be routed. The egress I-SBC removes the two new P-headers and verstat prior to sending the call to the next network.



Figure A 1: Assumption on TN Signing of NS/EP NGN-PS Calls

Signing of telephone numbers (i.e., Calling Party Numbers) as per [ATIS-1000074] is separate from SIP RPH signing. A separate SIP identity header is used for SIP RPH signing from that used for telephone number claims (i.e., SHAKEN assertion about Caller Identity). Both TN signing and SIP RPH signing would be performed for NS/EP NGN-PS calls, therefore, consistency between TN and SIP RPH signing will need to be ensured.

For SIP RPH signing, it is assumed that the originating Application Server shown in Figure A 1 would append a Resource Priority Header to the SIP INVITE after authenticating the NS/EP call request. The TN tagging function would then be applied to the INVITE. At the I-SBC, both the TN signing function and the RPH signing function (provided by the STI-AS in Figure A 1) would occur.

### Inter-Network NS/EP NGN-PS Calls

Figure A 2 shows an example reference architecture for an Inter-Network NS/EP NGN-PS Call with signed TN as per [ATIS-1000074] and signed SIP RPH as per the present document. The TN and SIP RPH is signed by the originating network as described in Section 1.1.1.

In the terminating network, when a call is received with a signed TN, it is sent to the STI-VS for verification. It is assumed that a Tagging function adds the verstat parameter (signifying TN-Validation-Passed) to emulate a successfully verified call. This verstat can be used by the terminating UE. A terminating A-SBC may remove the SHAKEN P-headers prior to sending the call to the terminating UE.



Figure A 2: TN Signing and SIP RPH Signing for Inter-Network NS/EP NGN-PS Calls

RPH verification is done similarly as for the TN verification; it is sent to the RPH verification function (provided by the RPH-VS function as part of the STI-VS).

# Example NS/EP NGN-PS Call Flow Scenarios

The following call scenarios are informative, and show how NS/EP NGN-PS Service Providers (e.g., GETS and WPS carriers) can use the rph PASSporT token. In these flows, a TN tagging function is shown as being performed at the TAS, and the STI functions are shown as being performed at a PASSporT AS.

## PASSporT Signing – NS/EP Originating Carrier

There are three types of NS/EP originating carriers: GETS Access Carriers, WPS Authenticating Carriers and GETS Authenticating Carriers. GETS Access Carriers are non-authenticating NS/EP carriers which provide NS/EP features based on a GETS Access Number (i.e., the call is forwarded to a GETS Authenticating Carrier for user authentication.

### GETS Access Carriers

GETS Access Carriers are not GETS Authenticating Carriers. These carriers recognize GETS Access Numbers and provide priority to GETS calls. As part of their functionality, they append Resource\_Priority: ets.0 to SIP INVITEs. Since they are not GETS Authenticating Carriers, they will use PASSporT Telephone Number (TN) signing.

NOTE: TN signing is not an NS/EP requirement.

The steps for the GETS Access Carrier flow shown in Figure A 3 are:

1. A user makes a call to a GETS number (e.g., 7101234567). The INVITE is sent to the P-CSCF.
2. The P-CSCF recognizes the 710 area code as a GETS call, and appends “Resource-Priority: ets.0” to the INVITE it sends into the network.
3. The TAS recognizes the 710 area code as a GETS call. If INVITE does not have an RPH, it appends “Resource-Priority: ets.0” to the INVITE. The TAS asserts the identity of the calling party by placing information in a PAI field. It then sends the INVITE to the network edge to forward the call to a GETS Authenticating Carrier.
4. The I-CSCF at the network edge routes the INVITE to a PASSporT Application Server for PASSporT signing.
5. Since the carrier is not a GETS Authenticating Carrier, the PASSporT AS performs a TN signing. It strips the P-Attestation-Indicator, P-Origination-Id and verstat fields from the INVITE and inserts the PASSporT (identified as TN PASSporT in the flow), and returns the INVITE to the I-CSCF.
6. The I-CSCF forwards the INVITE across the IPNNI.



Figure A 3: GETS Access Carrier PASSporT Signing Flow

### WPS Authenticating Carriers

WPS Authenticating Carriers recognize the WPS feature code and provide priority to WPS calls. As part of their functionality, they append Resource\_Priority: ets.0, wps.y to SIP INVITEs. These carriers will use PASSporT Resource Priority Header (RPH) signing and TN signing.

The steps for the WPS Authenticating Carrier flow shown in Figure A 4 are:

1. A user makes a WPS call using the \*272 feature code. The INVITE is sent to the P-CSCF.
2. The P-CSCF sends the INVITE to the TAS.
3. The TAS recognizes the \*272 feature code as a request for priority and queries the HSS if the call should be allowed. For a valid call, the TAS appends “Resource-Priority: ets.0, wps.y” to the INVITE. (Note that the y will be a value between 0 and 4 based on the priority of the WPS user.) The TAS asserts the identity of the calling party by placing information in a PAI field. It then sends the INVITE to the network edge to forward the call to the destination.
4. The I-CSCF at the network edge routes the INVITE to a PASSporT Application Server for PASSporT signing.
5. Since the carrier is a WPS Authenticating Carrier, the PASSporT AS performs a TN signing and an RPH signing. It strips the P-Attestation-Indicator, P-Origination-Id and verstat fields from the INVITE and inserts the PASSporTs (identified as TN PASSporT and RPH PASSporT“W” in the flow), and returns the INVITE to the I-CSCF.
6. The I-CSCF forwards the INVITE across the IPNNI.



Figure A 4: WPS Authenticating Carrier PASSporT Signing Flow

### GETS Authenticating Carriers

GETS Authenticating Carriers recognize the GETS access numbers, authenticate the user, and provide priority to GETS calls. As part of their functionality, they append Resource\_Priority: ets.0 to SIP INVITEs if RPH is not present. They will keep the ets.0, wps.y received from WPS carriers. These carriers will use PASSporT Resource Priority Header (RPH) signing and TN signing.

The steps for the GETS Authenticating Carrier flow shown in Figure A 5 are:

1. A user makes a call to a GETS number (e.g., 7101234567). The INVITE is sent to the P-CSCF.
2. The P-CSCF recognizes the 710 area code as a GETS call, and appends “Resource-Priority: ets.0” to the INVITE it sends into the network.
3. The S-CSCF routes the call to the GETS Authentication Server. The Authentication Server opens a two way media path with the user to obtain a PIN and destination number.
4. If the PIN is valid, the GETS Authentication Server modifies the calling and called parties as appropriate. It appends “Resource-Priority: ets.0” to the INVITE. The GETS Authentication Server asserts the identity of the (modified) calling party by placing information in a PAI field. It then sends the INVITE to the network edge to forward the call to the terminating carrier.
5. The I-CSCF at the network edge routes the INVITE to a PASSporT Application Server for PASSporT signing.
6. Since the carrier is a GETS Authenticating Carrier, the PASSporT AS performs a TN signing and an RPH signing. It strips the P-Attestation-Indicator, P-Origination-Id and verstat fields from the INVITE and inserts the PASSporTs (identified as TN PASSporT and RPH PASSporT“G” in the flow), and returns the INVITE to the I-CSCF.
7. The I-CSCF forwards the INVITE across the IPNNI.

The flow for the GETS Authentication carrier is applicable to all types of GETS calls including GETS Access Number (AN), Network Translation (NT) and Pseudo Destination Number (PDN) calls.

For a GETS AN call, the GETS Authentication Carrier will perform a TN signing based on the original calling party number and destination number entered during the PIN authentication process. For calls, requiring anonymity (e.g., NT and PDN calls), the GETS Authentication Carrier will replace the original calling party number with another number to make the call anonymous. The GETS Authentication Carrier will perform the TN signing based on the “anonymous” calling party number and the translated number.



Figure A 5: GETS Authenticating Carrier PASSporT Signing Flow

## GETS ACCESS CARRIER and GETS WPS Interaction with GETS Authenticating Carrier

Two flows are shown for this scenario. In the first, a TN PASSporT provided by a GETS Access Carrier is replaced with a TN PASSporT and an RPH PASSporT by the GETS Authenticating Carrier. In the second, a TN PASSporT and RPH PASSporT provided by a WPS Carrier is replaced by a TN PASSporT and an RPH PASSporT by the GETS Authenticating Carrier.

NOTE: In these flows, if the carrier receives a GET-AN (710) call with a TN Identity token that fails validation (e.g., the carrier validates the token at the IP-NNI edge before routing the GETS call across its domain to its authentication server), carrier-specific policies would apply in this case and other corner cases (e.g., a carrier may allow the GETS call to proceed to the authentication processing stage, or it may reject the call).

### GETS Access Carrier to GETS Authenticating Carrier

The steps for the flow between a GETS Access Carrier and GETS Authenticating Carrier are shown in Figure A 6, Figure A 7, and Figure A 8.

From Figure A 6:

1. A user makes a call to a GETS number (e.g., 7101234567). The INVITE is sent to the P-CSCF.
2. The P-CSCF recognizes the 710 area code as a GETS call, and appends “Resource-Priority: ets.0” to the INVITE it sends into the network.
3. The TAS recognizes the 710 area code as a GETS call. If INVITE does not have an RPH, it appends “Resource-Priority: ets.0” to the INVITE. The TAS asserts the identity of the calling party by placing information in a PAI field. It then sends the INVITE to the network edge to forward the call to a GETS Authenticating Carrier.
4. The I-CSCF at the network edge routes the INVITE to a PASSporT Application Server for PASSporT signing.
5. Since the carrier is not a GETS Authenticating Carrier, the PASSporT AS performs a TN signing. It strips the P-Attestation-Indicator, P-Origination-Id and verstat fields from the INVITE and inserts the PASSporT (identified as TN PASSporT in the flow), and returns the INVITE to the I-CSCF.
6. The I-CSCF forwards the INVITE across the IPNNI to the GETS Authenticating Carrier

Figure A 7 continues the flow:

1. The GETS Authentication Carrier’s I-CSCF checks to see if it owns the destination number (i.e., it is the terminating carrier) or if it needs to transit the INVITE to another carrier. It does this by querying the HSS on the destination number.
2. The query shows the GETS Authenticating Carrier is the terminating carrier. Since the PASSporT token does not cover the RPH, the I-CSCF can strip the RPH based on local policy. The I-CSCF can also insert an RPH based on local policy analyzing the destination number provided. The flow assumes the I-CSCF does not strip the RPH based on the destination number.
3. The I-CSCF passes the INVITE to the PASSporT AS to verify the TN PASSporT received. The PASSporT AS verifies the TN PASSporT, inserts validation information into a PAI field, and strips the PASSporT from the INVITE. The INVITE is returned to the I-CSCF
4. The I-CSCF forwards the INVITE to the S-CSCF, which then forwards the INVITE to the GETS Authentication Server

Figure A 8 continues the flow:

1. The Authentication Server opens a two way media path with the user to obtain a PIN and destination number.
2. If the PIN is valid, the GETS Authentication Server modifies the calling and called parties as appropriate. It appends “Resource-Priority: ets.0” to the INVITE. The GETS Authentication Server asserts the identity of the (modified) calling party by placing information in a PAI field. It then sends the INVITE to the network edge to forward the call to the terminating carrier.
3. The I-CSCF at the network edge routes the INVITE to a PASSporT Application Server for PASSporT signing.
4. Since the carrier is a GETS Authenticating Carrier, the PASSporT AS performs a TN signing and an RPH signing. It strips the P-Attestation-Indicator, P-Origination-Id and verstat fields from the INVITE and inserts the PASSporTs (identified as TN PASSporT\* [to distinguish it from the TN PASSporT initially received] and RPH PASSporT“G” in the flow), and returns the INVITE to the I-CSCF.
5. The I-CSCF forwards the INVITE across the IPNNI towards the terminating carrier.



Figure A 6: GETS Access Carrier to GETS Authenticating Carrier PASSporT Signing Flow (Part 1 of 3)

 

Figure A 7: GETS Access Carrier to GETS Authenticating Carrier PASSporT Signing Flow (Part 2 of 3)

 

Figure A 8: GETS Access Carrier to GETS Authenticating Carrier PASSporT Signing Flow (Part 3 of 3)

### WPS Carrier to GETS Authenticating Carrier

A WPS+GETS call (i.e., a call with a \*272 feature code and a GETS Access Number) is validated first by the WPS Carrier and then by the GETS Authentication Carrier. The steps for this flow between a WPS Carrier and GETS Authenticating Carrier is shown in Figure A 9, Figure A 10, and Figure A 11.

From Figure A 9:

1. A user makes a WPS call using the \*272 feature code. The INVITE is sent to the P-CSCF.
2. The P-CSCF sends the INVITE to the TAS.
3. The TAS recognizes the \*272 feature code as a request for priority and queries the HSS if the call should be allowed. For a valid call, the TAS appends “Resource-Priority: ets.0, wps.y” to the INVITE. (Note that the y will be a value between 0 and 4 based on the priority of the WPS user.) The TAS asserts the identity of the calling party by placing information in a PAI field. It then sends the INVITE to the network edge to forward the call to the destination.
4. The I-CSCF at the network edge routes the INVITE to a PASSporT Application Server for PASSporT signing.
5. Since the carrier is a WPS Authenticating Carrier, the PASSporT AS performs a TN signing and an RPH signing. It strips the P-Attestation-Indicator, P-Origination-Id and verstat fields from the INVITE and inserts the PASSporTs (identified as TN PASSporT and RPH PASSporT“W” in the flow), and returns the INVITE to the I-CSCF.
6. The I-CSCF forwards the INVITE across the IPNNI to the GETS Authenticating Carrier.

Figure A 10 continues the flow:

1. The GETS Authentication Carrier’s I-CSCF checks to see if it owns the destination number (i.e., it is the terminating carrier) or if it needs to transit the INVITE to another carrier. It does this by querying the HSS on the destination number.
2. The query shows the GETS Authenticating Carrier is the terminating carrier. The I-CSCF notes the INVITE has a TN PASSporT and an RPH PASSporT.
3. The I-CSCF passes the INVITE to the PASSporT AS to verify the TN PASSporT and RPH PASSporT received.
	1. If the TN PASSporT is not verified, the PASSporT AS follows local policy on what to do with the call. For example, the PASSporT AS could reject the call, or it could allow the call to proceed to the Authentication Platform.
	2. If the RPH PASSporT is not verified, the PASSporT AS follows local policy on what to do with the call. For example, it can strip the RPH from the call, or it call allow the RPH to remain, since a GETS Access Number is in the INVITE
	3. The PASSporT AS inserts information from the PASSporTs into a PAI field, and strips the PASSporTs from the INVITE. The INVITE is returned to the I-CSCF
4. The I-CSCF forwards the INVITE to the S-CSCF, which then forwards the INVITE to the GETS Authentication Server

Figure A 11 continues the flow:

1. The Authentication Server opens a two way media path with the user to obtain a PIN and destination number.
2. If the PIN is valid, the GETS Authentication Server modifies the calling and called parties as appropriate. It appends “Resource-Priority: ets.0” to the INVITE. The GETS Authentication Server asserts the identity of the (modified) calling party by placing information in a PAI field. It then sends the INVITE to the network edge to forward the call to the terminating carrier.
3. The I-CSCF at the network edge routes the INVITE to a PASSporT Application Server for PASSporT signing.
4. Since the carrier is a GETS Authenticating Carrier, the PASSporT AS performs a TN signing and an RPH signing. It strips the P-Attestation-Indicator, P-Origination-Id and verstat fields from the INVITE and inserts the PASSporTs (identified as TN PASSporT\* [to distinguish it from the TN PASSporT initially received] and RPH PASSporT“G” in the flow), and returns the INVITE to the I-CSCF.
5. The I-CSCF forwards the INVITE across the IPNNI towards the terminating carrier.



Figure A 9: WPS Carrier to GETS Authenticating Carrier PASSporT Signing Flow (Part 1 of 3)

 

Figure A 10: WPS Carrier to GETS Authenticating Carrier PASSporT Signing Flow (Part 2 of 3)

 

Figure A 11: WPS Carrier to GETS Authenticating Carrier PASSporT Signing Flow (Part 3 of 3)

## Transit Carrier PASSporT Flows

A non-NS/EP transit carrier must follow the rule to pass the PASSporT information unchanged. An NS/EP transit carrier may verify the PASSporT information provided to provide priority to the NS/EP call during transit. These flows are shown below.

### Non-NS/EP Transit Carrier

A non-NS/EP transit carrier will bypass the PASSporT AS and should send the Resource Priority Header unchanged, as shown in Figure A 12.

 

Figure A 12: Non-NS/EP Transit Carrier PASSporT Flow

### NS/EP Transit Carrier

An NS/EP transit carrier may want to verify an RPH PASSporT token before providing priority to the NS/EP call in its network.

A transit carrier may receive an RPH with a TN PASSporT. This case will occur when the transit carrier is used to send an INVITE from a GETS Access Carrier to a GETS Authentication Carrier. For this case, the carrier may remove the RPH if the “TO:” field does not contain a GETS Access Number. However, the transit carrier must pass the TN PASSporT unchanged. Figure A 13 shows the flow where a GETS Access Number is in the INVITE with a TN PASSporT.

 

Figure A 13: NS/EP Transit Carrier PASSporT Flow with TN PASSporT

A transit carrier can also receive an RPH with an RPH PASSporT. This can occur when:

* A WPS Carrier sends a WPS call towards a terminating carrier
* A WPS Carrier sends a WPS+GETS call towards a GETS Authentication Carrier
* A GETS Authentication Carrier sends a GETS call towards a terminating carrier

In these cases, the transit carrier may remove the RPH if the RPH PASSporT does not pass verification. However, the transit carrier must pass the RPH PASSporT unchanged. Figure A 14 shows the flow where the RPH PASSporT from a GETS Authentication Carrier is validated.



Figure A 14: NS/EP Transit Carrier PASSporT Flow with RPH PASSporT

## Terminating Carrier PASSporT Flows

### Non-NS/EP Terminating Carrier

A non-NS/EP terminating carrier can verify the TN PASSporT to provide Verstat information to the called party. Since an RPH PASSporT is present, the carrier should not send the INVITE to a 3rd party CVT for data analytics. This flow is shown in Figure A 15.

 

Figure A 15: Non-NS/EP Terminating Carrier PASSporT Flow

### NS/EP Terminating Carrier

An NS/EP terminating carrier can verify the RPH PASSporT for the Resource\_Priority field; and it may verify the TN PASSporT to provide verstat information to the called party. It shall not send the INVITE to a 3rd party CVT for data analytics. This flow is shown in Figure A 16.

NOTE: An NS/EP Terminating Carrier that receives an INVITE with an RPH PASSporT but no Resource\_Priority field may reinsert the RPH field in the INVITE after verifying the RPH PASSporT, based on local policy.

 

Figure A 16: NS/EP Terminating Carrier PASSporT Flow

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_-