STIR/SHAKEN in Emergency Communications and the Role of the Resource Priority Header

12/4/2019

Martin Dolly
Lead Member of Technical Staff
Core Network & Gov't/Regulatory Standards
ATIS – SIP Forum Co-Chair, STI-GC TC Chair,
and Director, SIP Forum
md3135@att.com

RPH Background

- [RFC 4412] defines the SIP “Resource-Priority” header field (RPH) for communications Resource-Priority
- The SIP RPH is used to influence prioritization afforded to communication sessions, including PSTN calls
  - For example, the SIP RPH is used to support priority services such as National Security/Emergency Preparedness (NS/EP) and Public Safety
- RPH namespaces assigned for specific application services are: “DSN,” “DRSN, ” “Q735,” “ETS”, “WPS” and “MCPTT.”

Problem Statement

- Lack of means to verify authenticity of information in received SIP RPHs
- SIP RPH namespace parameters could be spoofed or inserted by unauthorized entities
- Example: NS/EP Priority Services
  - Networks may drop SIP RPH with the “ETS” and “WPS” namespaces received from un-trusted networks due to lack of means to verify authenticity;
  - Impacting ability to support NS/EP Priority communications end-to-end across multiple service provider networks.
- Ability to verify authenticity of information in received SIP RPHs is needed to allow networks providing priority services to act on resource prioritization with confidence.

The PASSporT “shaken” extension

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. The SHAKEN PASSporT token would have the form given in the example below:

Protected Header

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

Payload

```
{
         "attest":"A",
         "dest":{"tn":["12125551213 "]},
         "iat":1443208345,
         "orig":{"tn":"12155551212"},
         "origid":"123e4567-e89b-12d3-a456-426655440000"
```

In addition to attestation, the unique origination identifier (“origid”) is defined as part of SHAKEN. This unique origination identifier should be a globally unique string corresponding to a Universally Unique Identifier (UUID) (RFC 4122). The origid will identify:

- Signing Carrier
- Carrier Customer/Access Carrier
- Entry Gateway

Signing RPH for NS/EP

- RFC 8443 defines a new JSON Web Token claim for "rph", which provides an assertion for information in ’SIP Resource-Priority’ header field.

- 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 MUST contain a "rph" claim, and any entities verifying the PASSporT object will be required to understand the "ppt" extension in order to process the PASSporT in question.

-

- A PASSPorT header with the "ppt“ included will look as follows:

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

Signing RPH for NS/EP

Specifically, the "rph" claim includes an assertion of the priority level of the user to be used for a given communication session.

The value of the "rph" claim is an Object with one or more keys.

Each key is associated with a JSON Array. These arrays contain Strings that correspond to the r-values indicated in the ’SIP Resource- Priority’ header field.

```
{
"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 [RFC8225]

using the full form of PASSPorT.

Authentication Service (Signing)

- Authentication service* derives the value of the “rph” claim by verifying authorization for Resource-Priority (e.g., verifying a calling user privilege for Resource-Priority based on its identity)
- An authority (signer) is only allowed to sign the content of a SIP RPH for which it has authority or delegated authority.

*Note: [RFC 4412] allows multiple “namespace “.” r-priority” pairs, either in a single SIP RPH or across multiple SIP RPHs. However, it is not necessary to sign all content of the SIP RPH or all SIP RPHs in a given SIP message. An authority is only responsible for signing content for which it has authority.

Verification Service

- Verified signature used as confirmation that Resource-Priority is authorized (e.g., calling party is authorized for Resource-Priority), and
- Used to provide priority treatment in accordance with local policy for the associated communication service (e.g., NS/EP and Public Safety).
- The Verification function needs only perform signature verification on the “rph” claim, in order to lower PDD

Deployment Assumptions for NS/EP

- RPH signing is only performed by the authenticating NS/EP service provider
- The authenticating NS/EP GETS service provider will remove TN Identity Header prior to performing NS/EP authentication
- NS/EP call information will never be provided to a 3rd party CVT for data analytics
- An NS/EP carrier may use the same certificates for signing RPH, as they use for TN signing
- Based on local policy, an NS/EP service provider may choose to honor NS/EP calls without a signed RPH or process with normal priority
  - This may change over time taking into account maturity of signed RPH deployments and knowledge of the adjacent carrier
- As with TN signing, RPH signing will not survive if there is interworking with the PSTN
- A new Verstat value will be required

RFC 7135 - Registering a SIP Resource Priority Header Field Namespace for Local Emergency Communications

This document creates the new Session Initiation Protocol (SIP) Resource Priority header (RPH) field namespace 'esnet' for local emergency usage and registers this namespace with IANA.

Below is an example of a Resource-Priority header field using the 'esnet' namespace:
Resource-Priority: esnet.0

The relative priority order for the 'esnet' namespace is as follows:

(lowest) esnet.0
esnet.1
esnet.2
esnet.3
(highest) esnet.4

Defined in the NENA i3 standard (NENA-STA-010). NENA-STA-010 specifies the use of "esnet.1" for 9-1-1 calls (i.e., emergency calls that traverse an ESInet) and "esnet.0" for callback calls (at least within the ESInet). "esnet.2" is defined for "Calls related to an incident in progress which are deemed critical" e.g., calls between agencies/PSAP authorities.   Uses for "esnet.3" and "esnet.4" are not defined.

Proposed PASSporT object and Claim for Emergency Services NETwork

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

```
{
"orig":{"tn":“CgPN"},
"dest":{["tn":“911 or URN-SOS"]},
"iat":1443208345,
"rph":{“ESorig":[“esnet,x"]}
}
```

```
 {
 "orig":{"tn":“EmergNet Num"},
 "dest":{["tn":“CgPN that originated emergency call"]},
 "iat":1443208345,
 "rph":{“EScallback":[“esnet,x"]}
 }
```

Deployment Assumptions for 911

- ESINET RPH Authentication is performed by the originating service provider, which can be the visiting SP for roaming scenarios
- ESINET RPH Verification may be provided to a 3rd party CVT for data analytics
- A SP may use the same certificates for signing RPH, as they use for TN signing
- Based on local policy, a ESINET or service provider may choose to honor 911 and callback calls without a signed RPH or process with normal priority
  - This may change over time taking into account maturity of signed PRH deployments and knowledge of the adjacent carrier
- As with TN signing, ESINET RPH signing will not survive if there is interworking with the PSTN
- An unique identifier will be defined to ID 911 calls made from non-registered mobile devices
- New Verstat values will be required

Signaling Verification

Verstat

- TN Validation Passed
- TN Validation Failed
- No TN Validation
- Future: same values above for CNAM

tel URI parameter in the P-Asserted-Identity or FROM header field in a SIP requests

P-Asserted-Identity: tel:+14085264000;verstat=TN-Validation-Passed

Security Considerations

- The Verification Function must drop a verstat tel URI parameter received in an INVITE
- If the terminating UE does not support the "verstat" parameter value, it must discard the parameter
- The terminating UE will act on the "verstat" parameter value, if the 200 (OK) response to the UE REGISTER includes a Feature-Caps header field, as specified in RFC 6809˚ [190], with a "+g.3gpp.verstat" header field parameter

Thank you.