Proposed PASSPorT Extension for Resource-Priority Authorization (draft-singh-stir-rph-00)

Ray P. Singh
rsingh@vencorelabs.com
Martin Dolly
md3135@att.com
Subir Das
sdas@vencorelabs.com
An Nguyen
An.p.nguyen@HQ.DHS.GOV

June 16, 2017

Overview

- **[draft-singh-stir-rph-00]: PASSPorT Extension for Resource-Priority Authorization**
  - Proposes a PASSPorT extension to convey cryptographically-signed assertion of authorization for communications “Resource-Priority”
  - Allows authorized service providers to sign and verify content of the SIP “Resource-Priority” header field specified in [RFC4412] and used to support priority services such as National Security /Emergency Preparedness (NS/EP) Priority Services and Public Safety.

Background

- [RFC 4412] defines the SIP “Resource-Priority” header field (RPH) for communications Resource-Priority
- The SIP RPH is used for priority routing and processing afforded to communication sessions,
  - 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”, “RTS”, “CRTS”, “ESNET”, “MCPTTQ” and “MCPTTP.”

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.

Solution Objective and Proposal

- Solution Objective
  - Leverage STIR [I-D.ietf-stir-rfc4474bis]: to sign and validate information populated in SIP RPHs
- Solution Proposal
  - Define STIR PASSPorT [I-D.ietf-stir-passport]: extension to sign and validate content of the RPH associated with the user
  - Stalkholders of specific priority services would specify how the STIR PASSPorT extension is used*

*Note: work is underway in ATIS/SIP Forum Task Force on IPNNI on use of STIR PASSPorT extension to support NS/EP Priority Services

Proposed PASSPorT Extension

- Define PASSPorT Claim: “ppt” value “rph”
- PASSPort with “rph” value will look like:

{“type”: “passport”,

“ppt”: “rph”,

“alg”: “ES256”,

“x5u”: https://www.example.org/cert.cer”}

Proposed PASSPorT Extension

- “rph” claim
  - Provides assertion of authorization, “auth”, for content of the SIP RPH based on [RFC 4412]: Resource-Priority: namespace “.” r-priority
- Example “rph” claim for SIP RPH with a “namespace “.” r-priority value of “ets.0”:

  {“orig”: {“tn” : “12155551212”},

  “dest”: “tn”: “12125551213”},

  “iat”: 1443208345,

  “rph”: {“auth”: “Resource-Priority: ets.0”}}

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).

Proposal

- It is proposed that IETF STIR accept proposed work item “draft-singh-stir-rph-00” to define a PASSPorT extension to convey cryptographically-signed assertion of authorization for communications “Resource-Priority.”