STIR WG
IETF-101

PASSPorT Extension for Resource-Priority Authorization

(draft-ietf-stir-rph-03)

11March, 2018

Ray P. Singh, Martin Dolly, Subir Das, and An Nguyen

Status Update

- Draft-ietf-stir-rph-00: PASSPorT Extension for Resource-Priority Authorization
  - Provides 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, civil Emergency and Public Safety.
  - The compact form of PASSporT is not specified (supported)
- Draft -00 was presented in IETF-99
- Draft -01 was presented in IETF-100
- Draft-02 was submitted in Jan, 2018 addressing all comments from WG Chair’s document shepherd write up
- Draft-03 was submitted in Feb, 2018 addressing AD and mailing list comments

Next Steps

- AD (Adam) stated that IETF last call will occur after IETF 101

Backup

List of Updates in Draft-ietf-stir-rph-03

Comment (in bold)	Proposed Resolution
Section 1: last paragraph “How the optional extension to PASSporT is used for real-time communications supported using SIP 'Resource-Priority' header field is defined in other documents and is outside the scope of this document.” **I assume these other documents are under development? If so, they should be cited here.**	Delete “is defined in other documents” Updated text: “How the optional extension to PASSporT is used for real-time communications supported using SIP ’Resource-Priority’ header field is outside the scope of this document.”

Section3: 2nd paragraph
A PASSPorT header with the "ppt“ included will look as follows:
{ "typ":"passport",
   "ppt":"rph",
    "alg":"ES256",
   "x5u":"https://www.example.org/cert.cer"}
Ideally, this would be either pretty-printed or canonicalized. Since it's too long to fit on a line in canonical form.
	Accepted the proposal and replaced the text with the following:
	
	{
	  "typ":"passport",
	  "ppt":"rph",
	  "alg":"ES256",
	  "x5u":"https://www.example.org/cert.cer"
	}

List of Updates in Draft-ietf-stir-rph-03

Comment (in bold)	Proposed Resolution

Section 3: Third paragraph
The following is an example "rph" claim for a SIP "Resource-Priority“ header field with a "namespace "." r-priority" value of "ets.0" and
with a "namespace "." r-priority" value of "wps.0".
{ "orig":{"tn":"12155551212"}
"dest":{["tn":"12125551213"]},
"iat":1443208345,
"rph":{"auth":["ets.0","wps.0"]}
 	
I recommend pretty-printing this. It's also missing a comma after the "orig" value, and the top-level structure is missing a closing brace. The value for "iat" needs to be enclosed in quotes.
 	
The NANPA has allocated NPA55501xx for example use, not NPA555xxxx, much of which remains assignable (cf <https://www.nationalnanpa.com/pdf/NRUF/ATIS-0300115.pdf>).
	Accepted the proposed changes:
	
	Updated text:
	
	The following is an example "rph" claim for a SIP ’Resource-Priority’ header field with a r-value ="namespace "." priority value" of "ets.0" and with another r-value= "namespace "." priority value" of "wps.0".
	
	{
	"orig":{"tn":"12155550112"},
	"dest":{["tn":"12125550113"]},
	"iat":"1443208345",
	"rph":{"auth":["ets.0", "wps.0"]}
	}

List of Updates in Draft-ietf-stir-rph-03

Comment (in bold)	Proposed Resolution
Section 4.1: 2nd paragraph **This example has a number of issues:** **In the Identity header field, the signed-identity-digest shouldn't be quoted.** **In the Identity header field, info is enclosed in <> rather than "".** **In the Identity header field, ppt is a token rather than a quoted string.** **The signed-identity-digest header needs to indicate a "typ" of "passport" rather than JWT, and it needs to include both a "ppt" and "x5u" field.** **The signed-identity-digest body should contain only the passport claim rather than a JSON object that itself contains a base64-encoded JWS header concatenated with a claim.** **I believe that, even when the body is included, values in the header and body need to be canonicalized (i.e., all on one line, no spaces, in alphabetical order, etc.)** **I would also recommend following the convention of indicating that line-wraps are only for readability, and including the header field name in the example. Putting all this together, I believe what you want is:**	Accepted the proposed changes: Updated Identity: Identity:eyJhbGciOiJFUzI1NiIsInBwdCI6I nJwaCIsInR5cCI6InBhc3Nwb3J0\ IiwieDV1IjoiaHR0cHM6Ly93d3cuZXhhbX BsZS5jb20vY2VydC5jZXIifQo.eyJkZ\ XN0Ijp7WyJ0biI6IjEyMTI1NTUwMTEzIl1 9LCJpYXQiOiIxNDQzMjA4MzQ1Iiwib3\ JpZyI6eyJ0biI6IjEyMTU1NTUwMTEyIn0sI nJwaCI6eyJhdXRoIjpbImV0cy4wIiw\ id3BzLjAiXX19Cg.s37S6VC8HM6Dl6YzJe QDsrZcwJ0lizxhUrA7f_98oWBHvo-cl\ - n8MIhoCr18vYYFy3blXvs3fslM_oos2P2D yw;info=<https://www.example.\ org/cert.cer>;alg=ES256;ppt=rph

List of Updates in Draft-ietf-stir-rph-03

Comment (in bold)	Proposed Resolution
Section 4.2: 2nd paragraph **This text is ambiguous about whether the validation indicates that the calling party is authorized to use the priorities indicated in the passport object, or the values in the SIP 'Resource-Priority' header field; and (taken on its face) implies the latter, when the intention here should clearly be the former.** **The text also needs to say something about comparing values in the claim to values in the 'Resource-Priority' header field, and what a mismatch might mean. The document says elsewhere that the signature might only cover some of the r-values, which makes it entirely possible that the 'Resource-Priority' field might contain more values than are signed. On the other hand, intermediaries might reasonably remove r-values as the call is processed. This probably means that those removed priorities should not be used, even if they are present in the passport. It seems reasonable to say that *typical* processing by a receiving party would be to take the *union* of all RPH passports that they trust, and *intersect* that with the priorities in 'Resource-Priority' header fields to get the actual priority or priorities to be applied to the call (subject to local policy).**	Accepted and updated the paragraph as follows: “ The verification service MUST extract the value associated with the "auth" key in a full form PASSPorT with a "ppt" value of "rph". If the signature validates, then the verification service can use the value of the "rph" claim as validation that the calling party is authorized for ’Resource-Priority’ as indicated in the claim. This value would in turn be used for priority treatment in accordance with local policy for the associated communication service. **If the signature validation fails, the verification service should infer that the calling party is not authorized for ’Resource-Priority’ as indicated in the claim. In such cases, the priority treatment for the associated communication service is handled as per the local policy.”** Also clarified texts in Section 3: last pargraph The credentials …. ….the signature must have authority over the **namespace of** the "rph" claim and there is only one authority per claim. **If r-values are added or dropped by the intermediaries along the path, intermediaries must generate a new "rph" header and sign the claim with its own authority.**

List of Updates in Draft-ietf-stir-rph-03

Comment (in bold)	Proposed Resolution
Section 7.2: Bullet items The authority that signs the token MUST have a secure method for authentication of the end user or the device. o The verification of the signature MUST include means of verifying that the signer is authoritative for the signed content of the SIP **It's not clear what authority is being claimed here. Is this supposed to mean something like "...verifying that the signer is authoritative for the originating tn in the PASSporT..."? Or "...authoritative for the resource priority namespace in the PASSporT?" Whatever the server is purportedly authoritative for needs to be clearly spelled out.**	Accepted and updated the bullet texts as follows: o An authority (signer) is only allowed to sign the content of a SIP 'Resource-Priority' header field for which it has the right authority. The authority that signs the token MUST have a secure method for authentication of the end user or the device. o The verification of the signature MUST include means of verifying that the signer is authoritative for the signed content of the resource priority namespace in the PASSporT.

List of Updates in Draft-ietf-stir-rph-03

Comment (in bold)	Proposed Resolution
Section 3: Comment from Christer { "orig":{"tn":"12155551212"} "dest":{["tn":"12125551213"]}, "iat":1443208345, "rph":{"auth":["ets.0","wps.0"]} …and the following text: "The credentials (e.g., authority responsible for authorizing Resource-Priority) used to create the signature must have authority over the "rph" claim…" **Since the claim also contains "orig", is the assumption that the signing entity always also has authority to assert the callers identity? I think it would be good to explicitly mention it.**	The claim is not on "orig" but on the SIP RPH namesapce. In response to one of the AD comments, this has been ~~refelcted~~ reflected. Section 3: Last paragraph "The credentials (e.g., authority responsible for authorizing Resource-Priority) used to create the signature must have authority **over the namespace** of the "rph" claim and there is only one authority per claim. The authority MUST use its credentials (i.e., CERT) associated with the specific service supported by the SIP **namespace in the claim**."