PASSporT

STIR Working Group
IETF95 - April 2016
Chris Wendt
Overview

- PASSporT is an evolution of the idea to use JWT/JWS based tokens and X.509 based digital signatures for asserting the identity of the initiator of personal communications

- STIR WG replacement for verified-token draft
PASSporT Header

• New MIME Media Type request: application/passport

• x5u header parameter - URI referring to public key certificate

• Example:

```json
{
    "typ":"passport",
    "alg":"RS256",
    "x5u":"https://cert.example.org/passport.crt"
}
```
PASSporT Payload

- JWT defined claims used in PASSporT
  - “iat” = date issued in “NumericDate” format
PASSporT Payload

• New claims requested in PASSporT
  • “otn”
  • “dtn”
  • “ouri”
  • “duri”
  • “mky”
PASSporT Payload - Identity Types

- PASSporT contains support for two types of identities
  - Telephone Numbers - “otn” and “dtn”
    - canonicalized based on 4474bis
  - URI - “ouri” and “duri”
    - RFC3986 defined URI (sip uri, jid, etc)
  - “o” and “d” refer to originating identity and destination identity
PASSporT Payload - Media Key

• “mky” - corresponds to a=fingerprint hash in SDP for DTLS-SRTP

• For example SDP that includes:

```
```

• The corresponding PASSporT Payload object would be:

```
{
  "iat":"1443208345",
  "otn":"12155551212",
  "duri":"sip:alice@example.com",
}
```
Multi-Party Communications

• Note for future, but should be straightforward to include all destination identities

• Does need some validation though
Extension to PASSporT base claims

• Two mechanisms:
  • Extending base claims (with base claims)
  • Defining a new set of claims (without base claims)
Extending base claims

• New header parameter:

  • “ppt” - a string that uniquely identifies a profile specification

• Example header:

```json
{
  "typ": "passport",
  "ppt": "foo",
  "alg": "RS256",
  "x5u": "https://tel.example.org/passport.crt"
}
```
Extending base claims

• Specifications that extend base claims MUST:
  • define new claims and register them per JWT/JWS
  • provide guidance on the application usage of how the new parameters are used
  • assume that some verifiers may not understand these profiles
Defining new set of claims

- Some may want to use the PASSporT digital signature mechanism but may want to create a completely new set of claims.

- Guidance is to create a new JWS “typ” with a corresponding MIME media type.

- Pre-pend “passport-“ to signify that is a type related to PASSporT.

- For example: “application/passport-foo”
Registering PASSporT extensions

- High level guidance for a way to register passport extensions
- Opinions?
Deterministic JSON serialization

- Borrows from JWK
- JSON object:
  - Remove whitespace
  - order claims in lexicographic order
- Example:

  ```json
  {
    "iat":1443208345,"otn":"1215551212","duri":"sip:alice@example.com",
  }
  ```
Examples

• Included examples with certificates and a reference token

• Any other examples people would like to see?
passport-02

- There is some syntax issues with 01, sorry :

- Will issue 02 within week to fix those and address any other comments out of this session