Rich Call Data

draft-ietf-stir-passport-rcd-10

STIR Working Group
IETF110

COMCAST

Overview

- Updates for draft-ietf-stir-passport-rcd-10 and draft-ietf-sipcore-callinfo-rcd-02
- Major update specific to integrity mechanism - will discuss in more detail

COMCAST

sipcore-callinfo-rcd-02

- Updated call-reason to suggested max length of 64 vs 160, still SHOULD
- Added a new MUST for URI usage. Allow only one level of URI references, URI referenced content (unless updated by future spec) MUST not have further URI references. Looking at current jCard properties, this seemed very reasonable and closes security holes.
- Added detailed guidance on multimedia file usage, including inclusion of image resolution and optionally bit depth/color information. This is for the inclusion of URL references for multiple resolutions and file formats for different end device display.
- Added cardinality (from jCard) mostly for convenience, relevant to including multiple image/logo
- Removed any MUST/SHOULD language for properties, didn’t seem to be useful, since we include only properties that are relevant to calling scenarios (please review)

COMCAST

stir-passport-rcd-10

- Major update to integrity/new modes definition for use of integrity
- Some clarification on “iss” third-party use case that “iss” is specifically meant to represent the distinction between first-party vs third-party use cases. Also changed reflection of “iss” in Organization field to Subject Name more generally.
- Added a security note regarding use of “rcd” claims as part of PASSporTs that are not “rcd” extensions that integrity rules and the use of JWTClaimsConstraints should be maintained for certificates used for signing other PASSporT types.
- Added a security considerations note to cover the use of I-D.housley-stir-enhance-rfc8226 for preventing the reuse of certificates for claims that were not authorized.

COMCAST

RCD integrity updates

- Got feedback as RCD is being implemented about a few issues with prior integrity mechanism.
- Integrity in previous iterations was a single digest over all of the RCD content therefore two problems:
  - if integrity is broken, it is not possible for verifier to determine which part of the RCD is broken (so it can at least display the parts that aren't broken)
  - with URI content hash as a single digest, the verifier is forced to download all of the URI references whether they need them or not. (problematic for providing multiple image options for different devices)
- So, a new flexible framework is defined that allows for multiple digests for specific objects within the RCD JSON to be integrity protected independently.
- To save bytes over the wire, RFC6901 JSON Pointer is used as a mechanism to identify the part of the JSON object that the digest is constructed from.

“rcdi” claim extension - example

```
{
  "orig": { "tn": "12025551000"},
  "dest": { "tn": ["12155551001"]},
  "iat": 1443208345,
  "rcd": {
    "nam": "Q Branch Spy Gadgets",
    "jcd": ["vcard",
    [ ["version",{},"text","4.0"],
      ["fn",{},"text","Q Branch"],
      ["org",{},"text","MI6;Q Branch Spy Gadgets"],
      ["photo",{},"uri","https://example.com/photos/q-256x256.png"],
      ["logo",{},"uri","https://example.com/logos/mi6-256x256.jpg"],
      ["logo",{},"uri","https://example.com/logos/mi6-64x64.jpg"],
    ] ]
  },
  "crn": "Rendezvous for Little Nellie",
  "rcdi": {
    "/jcd": "sha256-VNJDSNCJ12938918",
    "/jcd/1/3/3": "sha256-12938918VNJDSNCJ",
    "/jcd/1/4/3": "sha256-VNJDSNCJ12938918",
    “/jcd/1/5/3": "sha256-4049852730SFLGHL"
  }
}
```


COMCAST

“rcdi” claim extension - example

```
{
  "orig": {"tn": "12025551000"},
  "dest": {"tn": ["12155551001"]},
  "iat": 1443208345,
  "rcd": {
    "nam": "Q Branch Spy Gadgets",
    "jcl": "https://example.com/qbranch.json"
  },
  "crn": "Rendezvous for Little Nellie",
  "rcdi": {
    "/jcl": "sha256-VNJDSNCJ12938918",
    "/jcl/1/3/3": "sha256-12938918VNJDSNCJ",
    "/jcl/1/4/3": "sha256-VNJDSNCJ12938918",
    "/jcl/1/5/3": "sha256-4049852730SFLGHL"
  }
}

https://example.com/qbranch.json:
["vcard",
  [ ["version",{},"text","4.0"],
    ["fn",{},"text","Q Branch"],
    ["org",{},"text","MI6;Q Branch Spy Gadgets"],
    ["photo",{},"uri","https://example.com/photos/q-256x256.png"],
    ["logo",{},"uri","https://example.com/logos/mi6-256x256.jpg"],
    ["logo",{},"uri","https://example.com/logos/mi6-64x64.jpg"]
  ]
]
```


COMCAST

RCD integrity modes

Modes	No external URIs	Includes URI refs
Auth	1: No integrity req	2: RDC Integrity
Non-Auth	3: JWT Claim Const.	4: RCD Integ./JWT Claim Const.

- Discovered that the original 3 mode model proposed didn’t completely cover the right way of looking at when integrity is used.
- The new model has two explicit dimensions:
  - Whether there is URI referenced data in the “rcd” claim. This defines whether “rcdi” should be included.
  - Whether the signer is authoritative over the RCD being used (e.g. are they directly authoritative or has been delegated authority). This defines whether JWTClaimsConstraints should be included.

COMCAST

Questions?