Rich Call Data PASSporT extension

draft-ietf-stir-passport-rcd-04

STIR Working Group
IETF105

COMCAST

Overview of update

- Fairly large update with new concepts/reconsiderations
- Integrity is largest part essentially currently a first draft, wanted input
- Integrated integrity digest, a bit more comprehensive that we discussed, but we think for good reasons for specific use-cases
- Also Aligned more with call-info, provides a mechanism that is both:
  - more compatible with the intent of eCNAM which uses call-info
  - provides a path for compact form

call-info alignment

- call-info defines “icon”, “info”, “card”
- Question: should call-info/RCD be utilized together for two main cases
  - post-validation: extract out of identity header towards UE (e.g. eCNAM)
  - For compact-form, (i.e. canonicalize from display-name and call-info) define specific procedures and potentially more specifics for call-info
- Question: If we think this makes sense, should we have a specific effort/draft for aligning new call-info definitions?

COMCAST

Integrity claim

- Provides both a direct and indirect set of mechanisms for verification/ approval/policy enforcement of the contents of the rich call data
- “rcdi” - a digest of a canonical form of the “rcd” claim in its entirety, including concatenation of the contents of the URLs.
- Can use JWTConstraints to enforce use of “rcdi” claim and a specific digest value

COMCAST

Integrity claim

- Construction:
  - Pick algorithm for digest
  - Create canonicalized “rcd”
    - lexicographic order of keys
    - white space removal
    - concatenate the base64 encoded content of the resources pointed to by URLs in order of their appearance in re-ordered keys
    - create digest of resulting string

JWT Constraints

- In order to enforce the contents of the “rcd” in delegated and other indirect flows STIR certs including JWT Constraints can be used in the STIR certificate
- JWT Constraints would be as follows:
  - a "mustInclude" for the "rcd" claim
  - a "permittedValues" equal to the created "rcdi" claim value string.

COMCAST

Example of ‘rcdi’ claim construction

```
Example "rcd" claim with URL:
"rcd": { "nam" : "James Bond",
         "icon" : "https://example.org/james_bond.jpg"
       }

Example "rcd" input digest string:
{“icon":"https://example.org/james_bond.jpg","nam":"James Bond"};
  ONG##*NCCCDJK123...KLJASlkJlkjsadlf2e3

Example "rcdi" claim:
"rcdi":"sha256-u5AZzq6A9RINQZngK7T62em8M"
```


COMCAST

Example of “rcd" PASSporT with “nam” and “rcdi”

```
Protected Header
{
   "alg":"ES256",
   "typ":"passport",
   “ppt”:”rcd”,
   "x5u":"https://biloxi.example.org
        /biloxi.cer”
}
Payload
{
   "orig":{"tn":"12025551000"},
   "dest":{"tn":"12025551001"},
   “iat”:1443208345,
   “rcd":{"nam":"James Bond”},
   “rcdi":"sha256-H8BRh8j48O9oYatfu5AZzq6A9R6dQZngK7T62em8MUt1FLm52t+eX6xO"
}
```


COMCAST

Example of “rcd" PASSporT with “nam”, “jcl” and “rcdi”

```
Protected Header
{
   "alg":"ES256",
   "typ":"passport",
   “ppt”:”rcd”,
   "x5u":"https://biloxi.example.org
         /biloxi.cer”
}
Payload
{  "orig":{"tn":"12025551000"},
   "dest":{"tn":"12155551001"},
   "iat":1443208345,
   "rcd":{"nam":"James Bond”,"jcl":"https://example.org/james_bond.json"},
   "rcdi":"sha256-H8BRh8j48O9oYatfu5AZzq6A9R6dQZngK7T62em8MUt1FLm52t+eX6xO"
}
```


COMCAST

Eric/Ben/Russ questions/comments

- “personal communications”? This was a term we have used in RFC8225 at least
- Security issues with URL at terminating side of call? “inf” security of HTML? “jcd” and/or “jcl”?
- rcdi SHOULD vs MUST? (vs MAY) (and/or MAY for JWT Constraints)
- Why do we list three hash algorithms to pick from?
- Why do we canonicalize the “rcd” for creating the digest? 1. ordering of keys and URLs and order of the contents of the URLs, 2. will be useful for compact form
- “icn” vs. logo in “jcd”?
- 3rd party “rcd” is 😈 ?

COMCAST