draft-ietf-stir-passport-rcd-14

STIR Working Group
IETF 112 - 11/12/21

SOMOS®

Overview

- Had a checklist of items to fix based on comments from virtual meeting and a few issues identified on the list.

SOMOS®

Issues

- Comment from Ben: Section 5.1.4 says that “jcl” key is defined as an HTTPS URL, do we want other URI types allowed by callinfo-rcd draft.
- Would prefer to keep it to HTTPS URLs, so would make sure that callinfo-rcd draft also says this, but curious if others disagree with this?

SOMOS®

Issues

- clarify that like “nam”, “apn” represent intended default usage for simple display like text-only displays, but can also be reflected in the jcard for clients that know how to render richer information (do we need a specific mapping for jcard specific fields for nam and apn)
- remove the text/requirement that if “apn” is used then it can’t appear in the jcard
- added text: “"apn" MUST be used when it is the intent of the caller or signer to display the alternate presentation number even if "jcd" or "jcl" keys are present in a PASSporT with a "tel" key value.”

SOMOS®

Issues

- added to security consideration about the need for vetting of nam/apn

```
Whether its identities, alternate identities, images, logos,
physical addresses, all of the information contained in a
RCD PASSporT must follow some form of vetting in which the
authoritative entity or user of the information being signed
MUST follow an applicable policy of the eco-system using
RCD. This can be of many forms, depending on the setup and
constraints of the eco-system so is therefore out-of-scope
of this document. However, the general chain of trust that
signers of RCD PASSporT are either directly authoritative or
have been delegated authority through certificates using JWT
Claim Constraints and integrity mechanisms defined in this
and related documents is critical to maintain the integrity
of the eco-system utilizing this and other STIR related
specifications.
```

Issues

- clarify that “nam”, “apn” and all RCD data more generally has to be vetted, but in particular that apn number should be vetted similar to the calling telephone number
- added “How the signer determines that a user is authorized to present the number in question is a policy decision outside the scope of this document, however, the vetting of the alternate presentation number should follow the same level of vetting as telephone identities or any other information contained in an RCD PASSporT.”

SOMOS®

Issues

- fix consistency of logic of rules with Constraints
- In “rcd” usage:

```
The "permittedValues" for the "rcd" claim may optionally
contain multiple entries, to support the case where the
certificate holder is authorized to use different sets of
rich call data.

Only including "permittedValues" for "rcd" (with no
“mustInclude") provides the ability to either have no "rcd"
claim or only the set of constrained "permittedValues"
values for an included "rcd" claim.
```

- In “rcdi” usage:

```
For the case that there should always be both "rcd" and
"rcdi" values included in the "rcd" PASSporT, the
certificate JWT Claims Constraint MUST include both of the
following:

*  a "mustInclude" for the "rcd" claim, which simply
   constrains the fact that an "rcd" must be included if
   there is a "rcdi"

*  a "mustInclude" for the "rcdi" claim and a
   "permittedValues" equal to the created "rcdi" claim
   value string.

Note that optionally the "rcd" claims may be included in the
"permittedValues" however it is recognized that this may be
redundant with the "rcdi" permittedValues because the "rcdi"
digest will imply the content of the "rcd" claims
themselves.
```


SOMOS®

Issues

- specifically talk about “relying party” and verification of integrity for the data that that relying party specifically needs to consume, without implying that the PASSporT is “verified” if the integrity of URLs is not considered

- Ben mentioned this for security considerations “You can not separate the rcdi, if the URL is passed, you must make sure integrity is consistent to end party that is consuming URLS” but need to be careful to validate a practice of taking RCD passport and reconstructing it.

- Proposal from Russ: “if you fetch the URLs as a relying party then the integrity check needs to be considered for verification of the PASSporT”

- Proposed text on next page

SOMOS®

Issues

- Verification Rules

A PASSporT that uses claims defined in this specification, in order to have a successful verification outcome, MUST conform to the following:

* abide by all rules set forth in the proper construction of the claims

* abide by JWT Claims Constraint rules defined in [RFC8226] Section 8 or extended in [I-D.ietf-stir-enhance-rfc8226] if present in the certificate used to sign the PASSporT

* pass integrity verification using "rcdi" if present.

Consistent with the verification rules of PASSporTs more generally [RFC8225], if any of the above criteria is not met, the PASSporT verification should be considered a failed verification for all claims in the PASSporT.

In some middle box scenarios, a relying party may not have the need to validate content that is referenced by URIs (e.g. only wanting to validate base PASSporT info like "orig" and "dest" or other “rcd" info like "nam" or "apn"). In these scenarios, this procedure while not considered a full verification, can be performed without verifying the full integrity checks of URI referenced content.

Onward

- Any other issues to discuss?