

SHAKEN and Calling Name/RCD - Let's do this!

Chris Wendt

Overview

- Two Cases to support:
 - POCN - Plain old Calling Name
 - Rich Call Data - JCard, Logos, etc.
- draft-ietf-stir-passport-rcd-01
 - Proposes a new simple way to incorporate 'rcd' into PASSporT extensions
- This SHAKEN specific variant does assume a service provider specific case where the calling name is signed at the point of origination STI-AS. For 3rd party CNAM or terminating CNAM dips the default 'rcd' extension would apply.

POCN

- For POCN scenarios, the validation/verification of the calling name will utilize the 'rcd' claim with the 'nam' object set to however the calling name is represented in the INVITE. No plan to add any SIP mechanisms or standardize on one.
- Simply, using existing mechanisms for delivering calling name, the identity header will simply sign the exact string of the calling name and serve the ability to do a string compare with the 'rcd'/'nam'

Example POCN case

SIP INVITE

```
INVITE sip:+12155551213@biloxi.com SIP/2.0
Via: SIP/2.0/UDP
pc33.atlanta.com;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: "Bob" <sip:+12155551213@biloxi.com;
user=phone>
From: "Alice" <sip:+12155551212@atlanta.com;
user=phone>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 314159 INVITE
Date: Sat, 13 Nov 2015 23:29:00 GMT
Identity: "sv5CTo05KqpSmtHt3dcEiO/1CWTS
ZtnG3iV+1nmurLXV/HmtYNS7Ltrg9dlxkWzoeU
7d7OV8HweTTDobV3itTmgPwCFjaEmMyEI
3d7SyN21yNDo2ER/Ovgtw0Lu5csIppPqOgluX
ndzHbG7mR6Rl9BnUhHufVRbp51Mn3w0gfUs=";
info=<https://biloxi.example.org/
biloxi.cer>;alg=ES256;ppt="shaken"
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142
```

PASSporT

Protected Header

```
{
  "alg": "ES256",
  "typ": "passport",
  "ppt": "shaken",
  "x5u": "https://biloxi.example.org
        /biloxi.cer"
}
```

Payload

```
{
  "attest": "A"
  "dest": {"tn": ["12155551213"]}
  "iat": 1443208345,
  "orig": {"tn": "12155551212"},
  "origid": "123e4567-e89b-12d3-a456
            -426655440000",
  "rcd": {"nam": "Alice"}
}
```

Rich Call Data

- This is currently a bit open ended, but i think we can pretty much cover most of the “rich data” cases with RFC7095 jCard
- Name, Address, URI to logos, etc.
- One thing to think about is the security of the logo or other URIs
- Likely should add jCard as a standard case for ‘rcd’

Adding 'rcd' claim

- In latest draft, we introduced the mechanism of simply adding a 'rcd' claim to an existing PASSporT with extension.
- This avoids the need of, for example, creating a 'shaken+rcd' extension that would need to be specified.
- Calling Name is a common addition and as long as the Verification service understands 'rcd' it can process it. If it doesn't, it just ignores it and the calling name goes unverified. So, not adding any MUST requirements for verification services.
- Question: where do we define this in SHAKEN? Separate document? Add to 1000074 errata? (probably easiest if there is consensus)