shaken - where we are

Chris Wendt

COMCAST LABS

COMCAST

4474bis and Verified Token

- Had a meeting of the minds with editor of 4474bis to discuss a way forward to avoid splintering and zombie apocalypse
- Key points:
  - 4474bis never really had any opinions per say about certificate management
  - 4474bis was a bit confusing on the canonicalization, which probably didn’t help some of the confusions around scope
  - 4474bis-06 now has integrated the use of JWT claims as defined in verified-token draft
  - 4474bis-06 has the option to either include just the signature part or the full verified token in the identity header
  - 4474bis-07 will be targeted to normatively refer to verified-token for definition of claims

4474bis and Verified Token

- For 4474bis-06
  - everything moves into identity header
  - identity-info is depreciated and moved to “info” parameter
  - added “alg” to define crypto algorithm
  - optional “canon” parameter to provide base64 encoded header.claims, per verified-token

4474bis and Verified Token - extensibility

- Probably the least considered part of the current state of 4474bis-06 is extensibility
- We should provide opinions on this
- 4474bis-06 talks about spec as a parameter to Identity header
  - likely best perspective to think about this is for “cnam” claim
  - Something that we would want to be normative via verified token spec or a similar extension spec beyond verified token
  - Other extensibility could be industry specific or application specific and could be handled in many ways

Map between SIP message and VT claims

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/ICWTS
  ZtnG3iV+1nmurLXV/HmtyNS7Ltrg9dIxkWzoeU
  7d7OV8HweTTDobV3itTmgPwCFjaEmMyEI
  3d7SyN21yNDo2ER/Ovgtw0Lu5csIppPqOg1uX
  ndzHbG7mR6Rl9BnUhHufVRbp51Mm3w0gfUs=“;
  info=<https://biloxi.example.org/
  biloxi.cer>;alg=RS256
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142
```

VT header

```
{ "typ":"JWT",
     "alg":"RS256"
     “x5u”:"https://biloxi.example.org/
            biloxi.cer" }
```

VT claim

```
{ "orig":"12155551212",
     "term":"12155551213",
     "iat": “1443208345" }
```