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