Update on
JWS signed Vouchers

draft-ietf-anima-jws-voucher-01

Michael Richardson, Thomas Werner

mcr+ietf@sandelman.ca

thomas-werner@siemens.com

IETF 112

ANIMA Working Group

JWS Voucher

- RFC 8366 specifies CMS-signed JSON for Voucher artifacts
- This draft proposes JWS-signed JSON as another option
- Makes no YANG changes to RFC 8366

- Can be used by BRSKI RFC 8995
- BRSKI-PRM relies on JWS form factor

BRSKI: Bootstrapping of Remote Secure Key Infrastructure (RFC 8995)
BRSKI-PRM: BRSKI with Pledge in Responder Mode (draft-ietf-anima-brski-prm)
CMS: Cryptographic Message Syntax (RFC 5652)
JWS: JSON Web Signature (RFC 7515)
Voucher: A Voucher Artifact for Bootstrapping Protocols (RFC 8366)

JWS Options

- JWS Compact Serialization (RFC 7515 #3.1) is currently used
  - Encodes the three pieces (header.payload.signature) in Base64URL
  - This choice was arbitrary, but was driven by easier use with available libraries

- JWS JSON Serialization (RFC 7515 #3.2)
  - To be analyzed in conjunction with other needs … (OPC UA?)

OPC UA: Open Platform Communications Unified Architecture

JWS Voucher - History of changes

- Small improvements and fixes in writing and consistent usage of terms
  - Pledge voucher-request (PVR)
  - Registrar voucher-request (RVR)
  - Media-Type: application/voucher-jws+json
  - JWS (instead of JWT or JOSE)

- Updated References

JWS Voucher - Next Steps

- Further rework the draft (structure and application examples)
- Investigate 2nd JWS serialization option
- Circulate outcome on the mailing list for further discussion
- PoC implementation and interop in combination with BRSKI-PRM
- WG review appreciated

BRSKI-PRM: BRSKI with Pledge in Responder Mode (draft-ietf-anima-brski-prm)