Update on

JWS signed Vouchers

JWS signed Voucher Artifacts for Bootstrapping Protocols
draft-ietf-anima-jws-voucher-04

Michael Richardson, Thomas Werner
mcr+ietf@sandelman.ca
thomas-werner@siemens.com

IETF 114
ANIMA Working Group
Recap: 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 (CMS-signed JSON): A Voucher Artifact for Bootstrapping Protocols (RFC 8366)
Recap: JWS Options

- JWS JSON Serialization (RFC 7515 #3.2), concrete “General JWS JSON Serialization”
  - Switch from JWS Compact Serialization to “General JWS JSON Serialization”
  - Opens up the support of further use cases requiring more than one signature to the Voucher object
  - Multiple signatures are already supported by existing voucher form factors:
    - JSON-in-CMS - RFC 8366
    - CBOR-in-COSE_Sign - draft-ietf-anima-constrained-voucher
    - Voucher in JSON-in-JWS - draft-ietf-anima-jws-voucher (this draft)
      - should support same feature set as other Voucher forms (e.g. JSON-in-CMS), without limitation
Voucher Representation
General JWS JSON Serialization syntax and example

```json
{
    "payload": {
        "ietf-voucher:voucher": {
            "assertion": "logged",
            "serial-number": "0123456789",
            "nonce": "5742698422680472",
            "created-on": "2022-07-08T03:01:24.618Z",
            "pinned-domain-cert": "base64encodedvalue=="
        },
        "signatures": [
            {
                "protected": {
                    "x5c": [
                        "base64encodedvalue=="
                    ],
                    "alg": "ES256",
                    "typ": "voucher-jws+json"
                },
                "signature": "base64encodedvalue=="
            }
        ]
    }
}
```

Example Voucher Response

- Added optional header parameter „typ“
  (register with IANA, see section 6.1.1)
History of changes - draft-ietf-anima-jws-voucher-04

• Update chapter: "1. Introduction"

• Rework chapter: "3. Voucher Artifact with JSON Web Signature"

• Added optional header parameter "typ": "voucher-jws+json" and updated examples (PVR, RVR, Voucher)
JWS Voucher - Next Steps

• Finalize writing of this draft (content should be complete)
  • Alignment in BRSKI design team calls
  • Circulate outcome on the mailing list for further discussion

• Interop testing with others welcome 🎉
  • Could happen in combination with BRSKI-PRM interop

• WG review and shepherd appreciated

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

Discussion!  Questions? Feedback!

Thanks for your attention
Abbreviations, References

• 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 (JWS-signed JSON) JWS signed Voucher Artifacts for Bootstrapping Protocols (this draft, draft-ietf-anima-jws-voucher)
• Voucher (CMS-signed JSON) A Voucher Artifact for Bootstrapping Protocols (RFC 8366)
• PVR Pledge-voucher-request
• RVR Registrar-voucher-request