Update on
JWS signed Vouchers

draft-ietf-anima-jws-voucher-03

Michael Richardson, Thomas Werner

mcr+ietf@sandelman.ca

thomas-werner@siemens.com

IETF 113

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

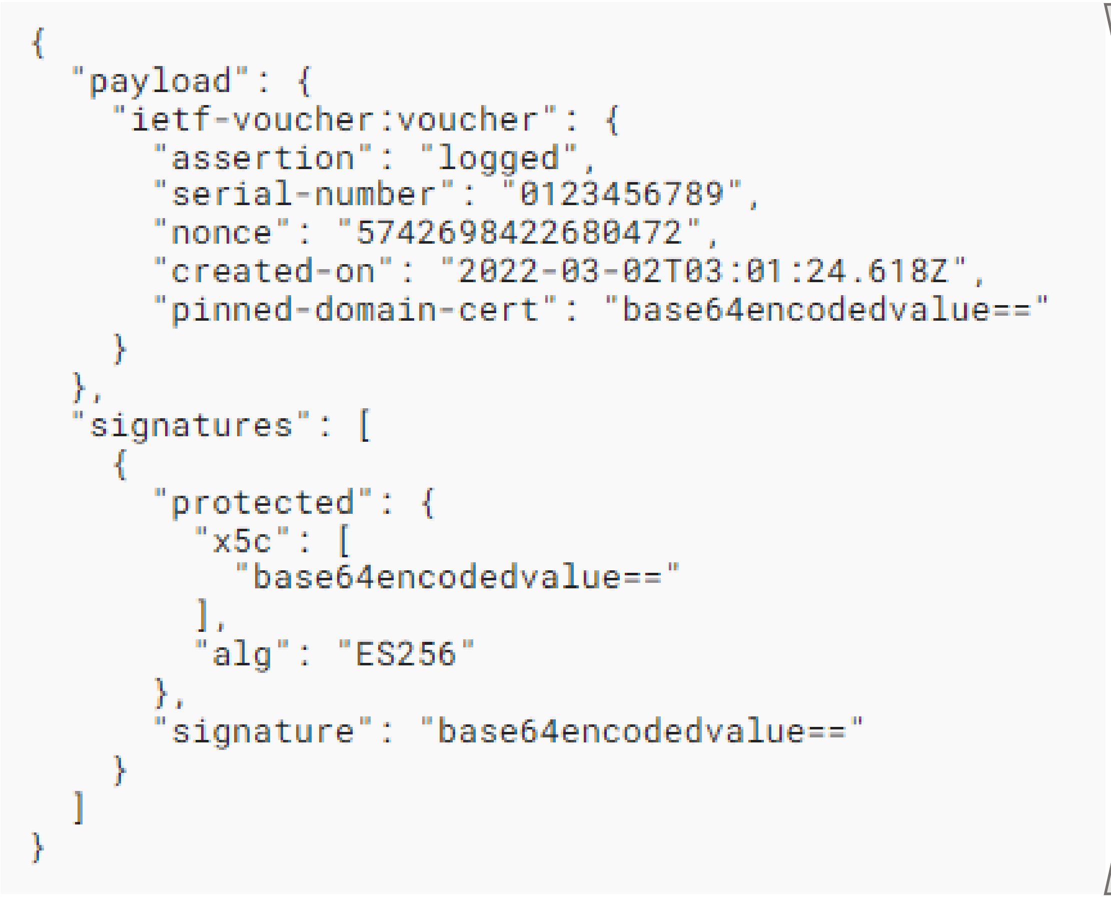
BRSKI: Bootstrapping of Remote Secure Key Infrastructure (RFC 8995)
BRSKI-PRM: BRSKI with Pledge in Responder Mode (draft-ietf-anima-brski-prm)
CMS: Cryptographic Message Syntax (RFC 5652)
JWS: JSON Web Signature (RFC 7515)
Voucher: A Voucher Artifact for Bootstrapping Protocols (RFC 8366)

JWS Options

- JWS Compact Serialization (RFC 7515 #3.1) was used initially
  - Encodes the three pieces (header.payload.signature) in Base64URL
  - This choice was arbitrary
  - To be replaced by “General JWS JSON Serialization”

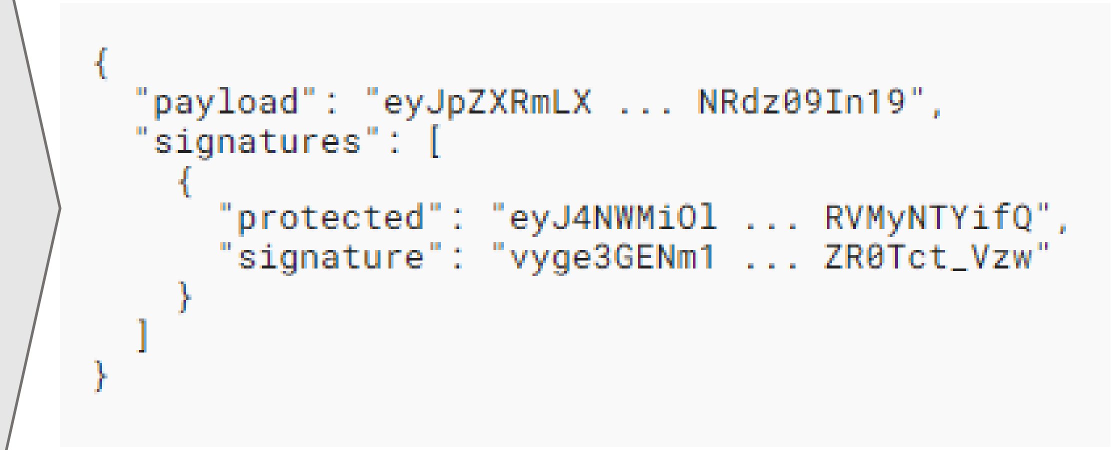
- JWS JSON Serialization (RFC 7515 #3.2), concrete “General JWS JSON Serialization”
  - Switch from JWS Compact Serialization to “General JWS JSON Serialization”
  - Opens up the support of further use cases requiring more than one signature to the Voucher object
  - Multiple signatures are already supported 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



```
{
  "payload": {
    "ietf-voucher:voucher": {
      "assertion": "logged",
      "serial-number": "0123456789",
      "nonce": "5742698422680472",
      "created-on": "2022-03-02T03:01:24.618Z",
      "pinned-domain-cert": "base64encodedvalue=="
    }
  },
  "signatures": [
    {
      "protected": {
        "x5c": [
          "base64encodedvalue=="
        ],
        "alg": "ES256"
      },
      "signature": "base64encodedvalue=="
    }
  ]
}
```

anima-jws-voucher.html#figure-1:
Voucher Representation in General JWS JSON Serialization Syntax



```
{
  "payload": "eyJpZXRmLX ... NRdz09In19",
  "signatures": [
    {
      "protected": "eyJ4NWMiOl ... RVMyNTYifQ",
      "signature": "vyge3GENm1 ... ZR0Tct_Vzw"
    }
  ]
}
```

anima-jws-voucher.html#figure-4:
Example Voucher Response

History of changes - draft-ietf-anima-jws-voucher-03

- Mainly switch from “JWS Compact Serialization” to “General JWS JSON Serialization”

- Include syntax and examples for Voucher request and response objects
  (PVR, RVR, Voucher)

JWS Voucher - Next Steps

- Further enhance description of “General JWS JSON Serialization”
- Alignment in BRSKI design team calls
- 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)

Abbreviations

- JWS - JSON Web Signature
- PVR - Pledge voucher-request
- RVR - Registrar voucher-request