

~~JOSE~~ JWS signed Vouchers

draft-ietf-anima-jws-voucher-00

Michael Richardson, Thomas Werner

mcr+ietf@sandelman.ca

Thomas Werner

thomas-werner@siemens.com

IETF 110

ANIMA Working Group

JWS Voucher

RFC8366 specifies CMS signed JSON

This draft proposes

- JWS signed JSON

Document renamed from JOSE-signed, to JWS-signed.

BRSKI: Bootstrapping of Remote Secure Key Infrastructures JOSE: JSON Object Signing and Encryption (RFC 7515)
CMS: Cryptographic message Syntax (RFC 5652)

Overview of Document

Table of Contents

1. Introduction	2
2. Terminology	3
3. JSON Web Signatures	3
3.1. Unprotected Header	4
3.2. Protected Header	4
4. Privacy Considerations	4
5. Security Considerations	4
6. IANA Considerations	4
6.1. Media-Type Registry	4
6.1.1. application/voucher-jose+json	4
7. Acknowledgements	5
8. Changelog	5
9. References	5
9.1. Normative References	5
9.2. Informative References	6
Appendix A. Examples	7
A.1. Example Voucher Request (from Pledge to Registrar) . . .	7
A.2. Example Parboiled Voucher Request (from Registrar to MASA)	9
A.3. Example Voucher Result (from MASA to Pledge, via Registrar)	12
Authors' Addresses	15

```
<CODE BEGINS> file "voucher_request_01-header.b64"
{
  "alg": "ES256",
  "x5c": [
    "MIIB2jCCAYCgAwIBAgIGAWeGdcSLMAoGCCqGSM49BAMCMD0xCzAJBg\
VBAYTAkFRMRUwEwYDVQQKDAxKaW5nSmluZ0NvcnAxZzAVBgNVBAMMDkppbm\
KaW5nVGZvdENBMCAxDTE4MTIxMjAzMjg1MVoYDzK5OTkxMjMxMjM1OTU5Wj\
SMQswCQYDVQQGEwJBUTEVMBMGA1UECgwMSmluZ0ppbmdb3JwMRMwEQYDVQ\
FEwowMTIzNDU2Nzg5MRcwFQYDVQQDDA5KaW5nSmluZ0RldmljZTBZMBMGB\
GSM49AgEGCCqGSM49AwEHA0IABMVGg8Z5pjf5jXnyrUrXyZ1kPgqBe3NXu1\
TADe+r/v6JzIHL355IgcHC3axpibqJM/bWRaEyjqcCJj4jJkowCujVTBTMC\
GCSsGAQQBg5SAgQfDB1tYXNhLXRlc3Quc2llbWVucy1idC5uZXQ6OTQ0Mz\
TBgNVHSUEDDAKBggrBgEFBQcDAjA0BgNVHQ8BAf8EBAMCB4AwCgYIKoZIZj\
EAWIDSAAwRQIgWtPzIIXY2ixRXJtExKEhhZda4X+EplZomEI2zA0dsjoCIQ\
3JpQmRXMGn/p4Bu9izii92eclTx4/04rlm7MyLqkhdA=="
  ]
}
<CODE ENDS>
```

Payload:

ichardson & Werner Expires 25 June 2021 [Page
Internet-Draft JOSE-voucher December

```
<CODE BEGINS> file "voucher_request_01-payload.b64"
{
  "ietf-voucher-request:voucher": {
    "created-on": "2020-10-22T02:37:39.000Z",
    "nonce": "eDs++/FuDHGUnRxN3E14CQ==",
    "serial-number": "0123456789"
  }
}
<CODE ENDS>
```

Signature:

```
<CODE BEGINS> file "voucher_request_01-signature.b64"
Vj9pyo43KDEq0e5tokwHpNhVM0uUkLCatwNqXfsCKH8GRQ2iTT2fqD39k40\
-7S-vheDHHuBHFSWb502EPwkda
<CODE ENDS>
```

Options

Uses the JWS **Compact** serialization.

- This format encodes the three pieces (protected headers, payload and signature) in Base64URL, appropriate for use in a URL.
- This choice was arbitrary, but was driven by being easier to use with available libraries.
 - This layer of Base64 encoding was not necessary, since HTTPS is 8-bit clean.

Conclusion

Adopted July 2021
Very short and sweet.

Makes no YANG changes to RFC8366.

`draft-ietf-anima-jws-voucher-00`