JOSE signed Vouchers

draft-richardson-anima-jose-voucher-00

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

IETF 110
ANIMA Working Group

JOSE Voucher

RFC8366 specificies CMS signed JSON

This draft proposes

- JOSE signed JSON

BRSKI: Bootstrapping of Remote Secure Key Infrastructures

JOSE: JSON Object Signing and Encryption (RFC 7515)
CMS: Cryptographic message Syntax (RFC 5652)

Overview of Document

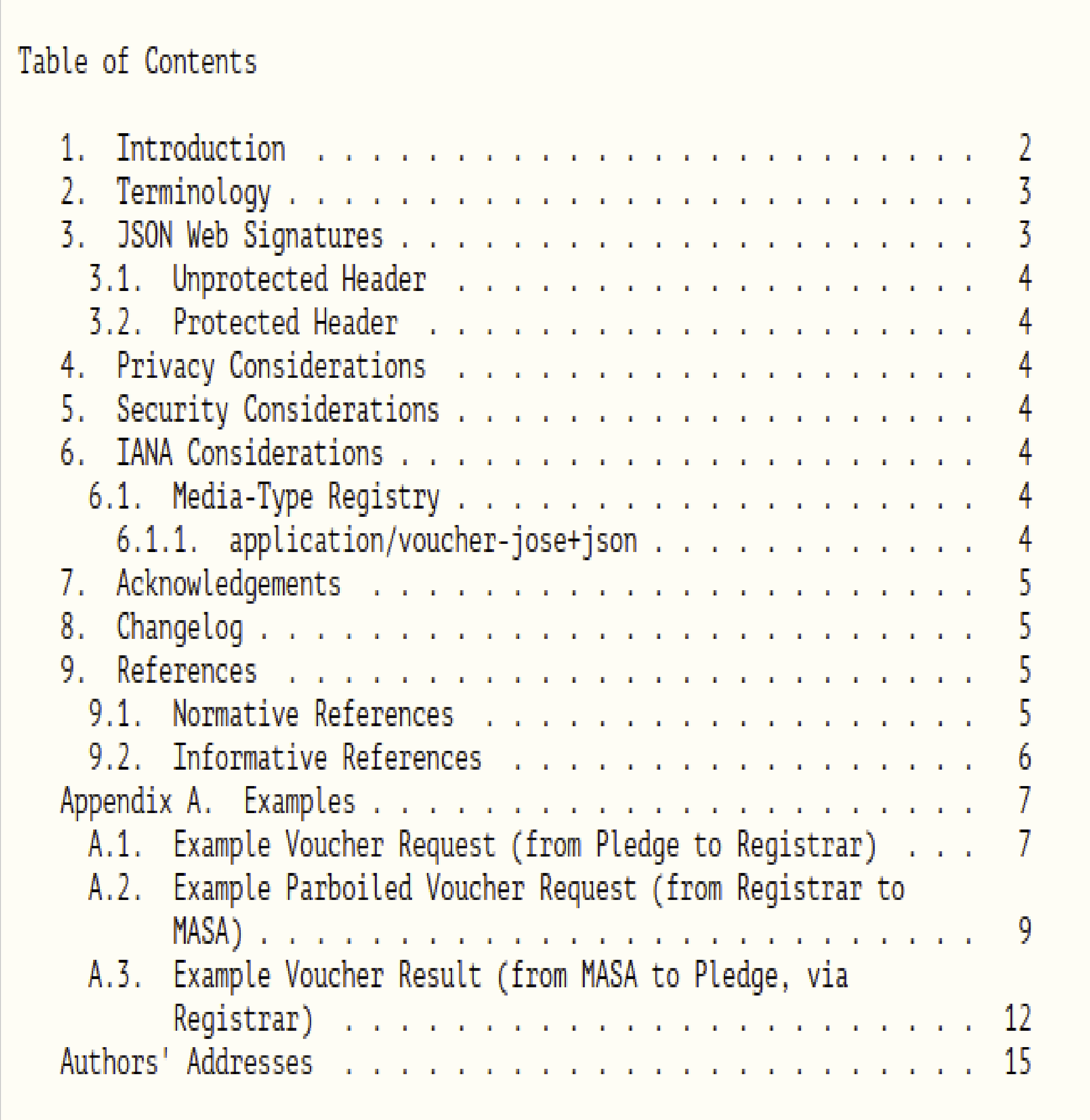
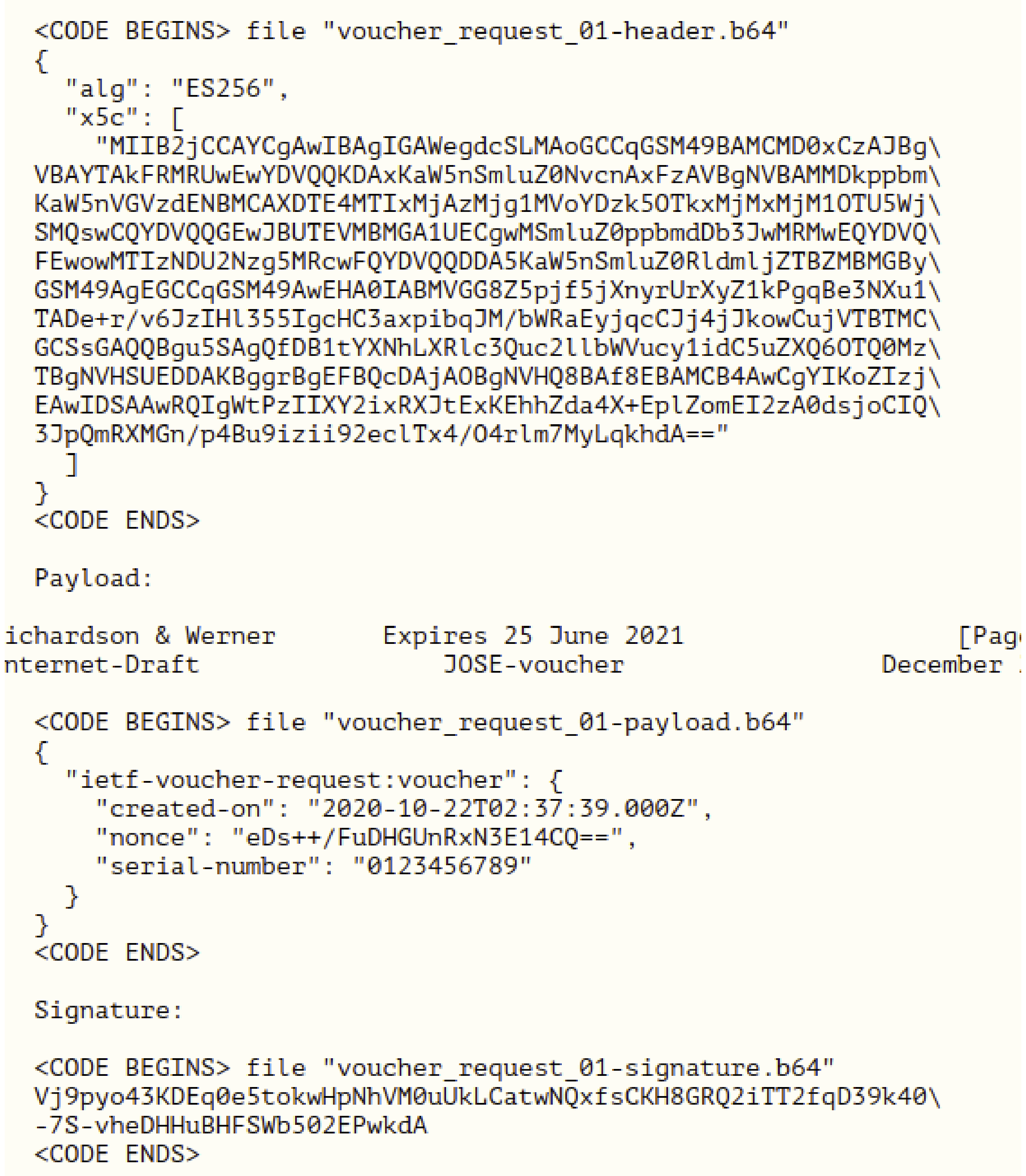


Table of Contents



```
 <CODE BEGINS> file "voucher_request_01-header.b64"
 {
   "alg": "ES256",
   "x5c": [
     "MIIB2jCCAYCgAwIBAgIGAWegdcSLMAoGCCqGSM49BAMCMD0xCzAJBg\
 VBAYTAkFRMRUwEwYDVQQKDAxKaW5nSmluZ0NvcnAxFzAVBgNVBAMMDkppbm\
 KaW5nVGVzdENBMCAXDTE4MTIxMjAzMjg1MVoYDzk5OTkxMjMxMjM1OTU5Wj\
 SMQswCQYDVQQGEwJBUTEVMBMGA1UECgwMSmluZ0ppbmdDb3JwMRMwEQYDVQ\
 FEwowMTIzNDU2Nzg5MRcwFQYDVQQDDA5KaW5nSmluZ0RldmljZTBZMBMGBy\
 GSM49AgEGCCqGSM49AwEHA0IABMVGG8Z5pjf5jXnyrUrXyZ1kPgqBe3NXu1\
 TADe+r/v6JzIHl355IgcHC3axpibqJM/bWRaEyjqcCJj4jJkowCujVTBTMC\
 GCSsGAQQBgu5SAgQfDB1tYXNhLXRlc3Quc2llbWVucy1idC5uZXQ6OTQ0Mz\
 TBgNVHSUEDDAKBggrBgEFBQcDAjAOBgNVHQ8BAf8EBAMCB4AwCgYIKoZIzj\
 EAwIDSAAwRQIgWtPzIIXY2ixRXJtExKEhhZda4X+EplZomEI2zA0dsjoCIQ\
 3JpQmRXMGn/p4Bu9izii92eclTx4/O4rlm7MyLqkhdA=="
   ]
 }
 <CODE ENDS>

 Payload:

ichardson & Werner        Expires 25 June 2021                [Pag
nternet-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

Adopt?
Very short and sweet.

`draft-richardson-anima-jose-voucher-00`