Workgroup: anima Working Group
Internet-Draft:
draft-ietf-anima-jws-voucher-00
Updates: RFC8366 (if approved)
Published: 25 July 2021
Intended Status: Standards Track
Expires: 26 January 2022
Authors: M. Richardson
Sandelman Software Works
T. Werner
Siemens

# JWS signed Voucher Artifacts for Bootstrapping Protocols

## Abstract

RFC8366 defines a digital artifact called voucher as a YANG-defined JSON document that has been signed using a Cryptographic Message Syntax (CMS) structure. This memo introduces a variant of the voucher structure in which CMS is replaced by the JSON Object Signing and Encryption (JOSE) mechanism described in RFC7515 to better support use-cases in which JOSE is preferred over CMS.

In addition to explaining how the format is created, MIME types are registered and examples are provided.

## Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 26 January 2022.

## Copyright Notice

carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

**Table of Contents**



## 1. Introduction

"A Voucher Artifact for Bootstrapping Protocols", [RFC8366] describes a voucher artifact used in "Bootstrapping Remote Secure Key Infrastructure" [BRSKI] and "Secure Zero Touch Provisioning" [SZTP] to transfer ownership of a device to from a manufacturer to an owner. That document defines the base YANG module, and also the initial serialization to JSON [RFC8259], with a signature provided by [RFC5652].

Other work, [I-D.ietf-anima-constrained-voucher] provides a mapping of the YANG to CBOR [RFC8949] with a signature format of COSE [RFC8812].

This document provides an equivalent mapping of JSON format with the signature format in JOSE format [RFC7515]. The encoding specified in this document is required for [I-D.ietf-anima-brski-async-enroll] and may be required and/or preferred in other use-cases, for example when JOSE is already used in other parts of the use-case, but CMS is not.

This document does not extend the YANG definition of [RFC8366] at all, but accepts that other efforts such as [I-D.richardson-anima-voucher-delegation], [I-D.friel-anima-brski-cloud], and [I-D.ietf-anima-brski-async-enroll] do. This document supports signing any of the extended schemas defined in those documents and any new documents that may appear after this one.

With the availability of different encoded vouchers, it is up to an industry specific application statement to indicate/decide which voucher format is to be used. There is no provision across the different voucher formats that a receiver could safely recognize which format it uses unless additional context is provided. For example, [BRSKI] provides this context via the MIME-Type for the voucher payload.

This document should be considered an Update to [RFC8366] in the category of "See Also" as per [I-D.kuehlewind-update-tag].

## 2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

## 3. JSON Web Signatures

[RFC7515] defines two serializations: the JWS Compact Serialization and the JWS JSON Serialization. The two serializations are mostly equivalent, and the JWS Compact Serialization (JWT) format has better library support in web frameworks, so this document restricts itself to that choice.

The [RFC8366] JSON structure consists of a nested map, the outer part of which is:

```
{ "ietf-voucher:voucher" : { some inner items }}
```

this is considered the JSON payload as described in [RFC7515] section 3.

The JSON Compact Serialization is explained in section 3.1 or section 7.1, and works out to:

```
BASE64URL(UTF8(JWS Protected Header)) || '.' ||
BASE64URL(JWS Payload) || '.' ||
BASE64URL(JWS Signature)
```

Note that this results in a long base64 content (with two interspersed dots). When using HTTPS, the voucher is transmitted in base64 format, even though HTTP can accommodate binary content. This is done to be most convenient for available JWT libraries, and for humans who are debugging.

There are a number of attributes. They are:

### 3.1. Unprotected Header

There is no unprotected header in the Compact Serialization format.

### 3.2. Protected Header

The standard "typ" and "alg" values described in [RFC7515] are expected in the protected headers.

It remains to be determined (XXX), what values, if any, should go into the "typ" header, as in the [BRSKI] use cases, there are additional HTTP MIME type headers to indicate content types.

The "alg" should contain the algorithm type such as "ES256".

If PKIX [RFC5280] format certificates are used then the [RFC7515] section 4.1.6 "x5c" certificate chain SHOULD be used to contain the certificate and chain. Vouchers will often need all certificates in the chain, including what would be considered the trust anchor certificate because intermediate devices (such as the Registrar) may need to audit the artifact, or end systems may need to pin a trust anchor for future operations. This is consistent with [BRSKI] section 5.5.2.

## 4. Privacy Considerations

The Voucher Request reveals the IDevID of the system that is on-boarding.

This request occurs over HTTPS, however the Pledge to Registrar transaction is over a provisional TLS session, and it is subject to disclosure via by a Dolev-Yao attacker (a "malicious messenger") [onpath]. This is explained in [BRSKI] section 10.2.

The use of a JWS header brings no new privacy considerations.

## 5. Security Considerations

The issues of how [RFC8366] vouchers are used in a [BRSKI] system is addressed in section 11 of that document. This document does not change any of those issues, it just changes the signature technology used for vouchers and voucher requests.

[SZTP] section 9 deals with voucher use in Secure Zero Touch Provisioning, and this document also makes no changes to security.

## 6. IANA Considerations

### 6.1. Media-Type Registry

This section registers the 'application/voucher-jws+json' in the "Media Types" registry.

#### 6.1.1. application/voucher-jws+json

Type name: application
Subtype name: voucher-jwt+json
Required parameters: none
Optional parameters: none
Encoding considerations: JWS+JSON vouchers are JOSE objects signed with one signer.
Security considerations: See Security Considerations, Section
Interoperability considerations: The format is designed to be broadly interoperable.
Published specification: THIS RFC.
Applications that use this media type: ANIMA, 6tisch, and other zero-touch imprinting systems
Additional information:
Magic number(s): None
File extension(s): .vjj
Macintosh file type code(s): none
Person & email address to contact for further information: IETF ANIMA WG
Intended usage: LIMITED
Restrictions on usage: NONE
Author: ANIMA WG
Change controller: IETF
Provisional registration? (standards tree only): NO

## 7. Changelog

*Added adoption call comments from Toerless. Changed from [RFCxxxx] to [THING] style for some key references.

## 8. References

### 8.1. Normative References

**[BRSKI]** Pritikin, M., Richardson, M., Eckert, T., Behringer, M., and K. Watsen, "Bootstrapping Remote Secure Key Infrastructure (BRSKI)", RFC 8995, DOI 10.17487/RFC8995, May 2021, <https://www.rfc-editor.org/info/rfc8995>.

**[RFC2119]** Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

**[RFC7515]** Jones, M., Bradley, J., and N. Sakimura, "JSON Web Signature (JWS)", RFC 7515, DOI 10.17487/RFC7515, May 2015, <https://www.rfc-editor.org/info/rfc7515>.

**[RFC8174]** Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

**[RFC8259]** Bray, T., Ed., "The JavaScript Object Notation (JSON) Data Interchange Format", STD 90, RFC 8259, DOI 10.17487/RFC8259, December 2017, <https://www.rfc-editor.org/info/rfc8259>.

**[RFC8366]** Watsen, K., Richardson, M., Pritikin, M., and T. Eckert, "A Voucher Artifact for Bootstrapping Protocols", RFC 8366, DOI 10.17487/RFC8366, May 2018, <https://www.rfc-editor.org/info/rfc8366>.

**[SZTP]** Watsen, K., Farrer, I., and M. Abrahamsson, "Secure Zero Touch Provisioning (SZTP)", RFC 8572, DOI 10.17487/RFC8572, April 2019, <https://www.rfc-editor.org/info/rfc8572>.

### 8.2. Informative References

**[I-D.friel-anima-brski-cloud]** Friel, O., Shekh-Yusef, R., and M. Richardson, "BRSKI Cloud Registrar", Work in Progress, Internet-Draft, draft-friel-anima-brski-cloud-04, 6 April 2021, <https://www.ietf.org/archive/id/draft-friel-anima-brski-cloud-04.txt>.

**[I-D.ietf-anima-brski-async-enroll]** Fries, S., Brockhaus, H., Lear, E., and T. Werner, "Support of asynchronous Enrollment in BRSKI (BRSKI-AE)", Work in Progress, Internet-Draft, draft-ietf-anima-brski-async-enroll-03, 24 June 2021, <https://www.ietf.org/archive/id/draft-ietf-anima-brski-async-enroll-03.txt>.

**[I-D.ietf-anima-constrained-voucher]** Richardson, M., Stok, P. V. D., Kampanakis, P., and E. Dijk, "Constrained Voucher Artifacts for Bootstrapping Protocols", Work in Progress, Internet-Draft, draft-ietf-anima-constrained-voucher-12, 11 July 2021, <https://www.ietf.org/archive/id/draft-ietf-anima-constrained-voucher-12.txt>.

**[I-D.kuehlewind-update-tag]**
Kuehlewind, M. and S. Krishnan, "Definition of new tags for relations between RFCs", Work in Progress, Internet-Draft, draft-kuehlewind-update-tag-04, 12 July 2021, <https://www.ietf.org/archive/id/draft-kuehlewind-update-tag-04.txt>.

**[I-D.richardson-anima-voucher-delegation]** Richardson, M. and W. Pan, "Delegated Authority for Bootstrap Voucher Artifacts", Work in Progress, Internet-Draft, draft-richardson-anima-voucher-delegation-03, 22 March 2021, <https://www.ietf.org/archive/id/draft-richardson-anima-voucher-delegation-03.txt>.

**[onpath]** "can an on-path attacker drop traffic?", n.d., <https://mailarchive.ietf.org/arch/msg/saag/m1r9uo4xYznOcf85Eyk0Rhut598/>.

**[RFC5280]** Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

**[RFC5652]** Housley, R., "Cryptographic Message Syntax (CMS)", STD 70, RFC 5652, DOI 10.17487/RFC5652, September 2009, <https://www.rfc-editor.org/info/rfc5652>.

**[RFC8792]** Watsen, K., Auerswald, E., Farrel, A., and Q. Wu, "Handling Long Lines in Content of Internet-Drafts and RFCs", RFC 8792, DOI 10.17487/RFC8792, June 2020, <https://www.rfc-editor.org/info/rfc8792>.

**[RFC8812]** Jones, M., "CBOR Object Signing and Encryption (COSE) and JSON Object Signing and Encryption (JOSE) Registrations for Web Authentication (WebAuthn) Algorithms", RFC 8812, DOI 10.17487/RFC8812, August 2020, <https://www.rfc-editor.org/info/rfc8812>.

**[RFC8949]** Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", STD 94, RFC 8949, DOI 10.17487/RFC8949, December 2020, <https://www.rfc-editor.org/info/rfc8949>.

## Appendix A. Examples

These examples are folded according to [RFC8792] Single Backslash rule.

### A.1. Example Voucher Request (from Pledge to Registrar)

The following is an example request sent from a Pledge to the Registrar. This example is from the Siemens reference Registrar system.

<CODE BEGINS> file "voucher_request_01.b64"

```
eyJhbGciOiAiRVMyNTYiLCAieDVjIjogWyJNSUlCMmpDQ0FZQ2dBd0lCQWd\
R0FXZWdkY1NMTUFvR0NDcUdTTTQ5QkFNQ01EMHhDekFKQmdOVkJBWVRBa0Z\
TVJVd0V3WURWUVFLREF4S2FXNW5TbWx1WjBOdmNuQXhGekFWQmdOVkJBTU1\
a3BwYm1kS2FXNW5WR1Z6ZEVOQk1DQVhEVEU0TVRJeE1qQXpNamcxTVZvWUR\
azVPVGt4TWpNeE1qTTFPVFU1V2pCU01Rc3dDUVlEVlFRR0V3SkJVVEVWTUJ\
R0ExVUVDZ3dNU21sdVowcHBibWREYjNKd01STXdFUVlEVlFRRkV3b3dNVEl\
TkRVMk56ZzVNUmN3RlFZRFZRUUREQTVLYVc1blNtbHVaMFJsZG1salpUQlp\
Qk1HQnlxR1NNNDlBZ0VHQ0NxR1NNNDlBd0VIQTBJQUJNVkdHOFo1cGpmNWp\
bnlyVXJYeVoxa1BncUJlM05YdTFkVEFEZStyL3Y2SnpJSGwzNTVJZ2NIQzN\
eHBpYnFKTS9iV1JhRXlqcWNDSmo0akprb3dDdWpWVEJUTUN3R0NTc0dBUVF\
Z3U1U0FnUWZEQjF0WVhOaExYUmxjM1F1YzJsbGJXVnVjeTFpZEM1dVpYUTZ\
VFEwTXpBVEJnTlZIU1VFRERBS0JnZ3JCZ0VGQlFjREFqQU9CZ05WSFE4QkF\
OEVCQU1DQjRBd0NnWUlLb1pJemowRUF3SURTQUF3UlFJZ1d0UHpJSVhZMml\
UlhKdEV4S0VoaFpkYTRYK0VwbFpvbUVJMnpBMGRzam9DSVFDM0pwUW1SWE1\
bi9wNEJ1OWl6aWk5MmVjbFR4NC9PNHJsbTdNeUxxa2hkQT09Il19.eyJpZX\
mLXZvdWNoZXItcmVxdWVzdDp2b3VjaGVyIjogeyJjcmVhdGVkLW9uIjogIj\
wMjAtMTAtMjJUMDI6Mzc6MzkuMDAwWiIsICJub25jZSI6ICJlRHMrKy9GdU\
IR1VuUnhOM0UxNENRPT0iLCAic2VyaWFsLW51bWJlciI6ICIwMTIzNDU2Nz\
5In19.Vj9pyo43KDEq0e5tokwHpNhVM0uUkLCatwNQxfsCKH8GRQ2iTT2fq\
39k40M-7S-vheDHHuBHFSWb502EPwkdA
<CODE ENDS>
```

It contains the following three parts:

Header:

<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:

<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>

### A.2. Example Parboiled Voucher Request (from Registrar to MASA)

The term parboiled refers to food which is partially cooked. In [BRSKI], the term refers to a voucher-request which has been received by the Registrar, and then has been processed by the Registrar ("cooked"), and is now being forwarded to the MASA.

The following is an example request sent from the Registrar to the MASA. This example is from the Siemens reference Registrar system. Note that the previous voucher request can be seen in the payload as "prior-signed-voucher-request".

<CODE BEGINS> file "parboiled_voucher_request_01.b64"

```
eyJhbGciOiJFUzI1NiIsIng1YyI6WyJNSUlCb3pDQ0FVcWdBd0lCQWdJR0F\
MGVMdUlGTUFvR0NDcUdTTTQ5QkFNQ01EVXhFekFSQmdOVkJBb01DazE1UW5\
emFXNWxjM014RFRBTEJnTlZCQWNNQkZOcGRHVXhEekFOQmdOVkJBTU1CbFJ\
YzNSRFFUQWVGdzB4T1RBNU1URXdNak0zTXpKYUZ3MHlPVEE1TVRFd01qTTN\
ekphTUZReEV6QVJCZ05WQkFvTUNrMTVRblZ6YVc1bGMzTXhEVEFMQmdOVkJ\
Y01CRk5wZEdVeExqQXNCZ05WQkFNTUpWSmxaMmx6ZEhKaGNpQldiM1ZqYUd\
eUlGSmxjWFZsYzNRZ1UybG5ibWx1WnlCTFpYa3dXVEFUQmdjcWhrak9QUUl\
QmdncWhrak9QUU1CQndOQ0FBVDZ4VnZBdnFUejFaVWl1TldoWHBRc2thUHk\
QUhIUUx3WGlKMGlFTHQ2dU5QYW5BTjBRbldNWU8vMENERWpJa0JRb2J3OFl\
cWp0eEpIVlNHVGo5S09veWN3SlRBVEJnTlZIU1VFRERBS0JnZ3JCZ0VGQlF\
REhEQU9CZ05WSFE4QkFmOEVCQU1DQjRBd0NnWUlLb1pJemowRUF3SURSd0F\
UkFJZ1lyMkxmcW9hQ0tERjRSQWNNbUppK05DWnFkU2l1VnVnSVNBN09oS1J\
M1lDSUR4blBNTW5wWEFNVHJQSnVQV3ljZUVSMTFQeEhPbiswQ3BTSGkycWd\
V1giLCJNSUlCcERDQ0FVbWdBd0lCQWdJR0FXMGVMdUgrTUFvR0NDcUdTTTQ\
QkFNQ01EVXhFekFSQmdOVkJBb01DazE1UW5WemFXNWxjM014RFRBTEJnTlZ\
QWNNQkZOcGRHVXhEekFOQmdOVkJBTU1CbFJsYzNSRFFUQWVGdzB4T1RBNU1\
RXdNak0zTXpKYUZ3MHlPVEE1TVRFd01qTTNNekphTURVeEV6QVJCZ05WQkF\
TUNrMTVRblZ6YVc1bGMzTXhEVEFMQmdOVkJBY01CRk5wZEdVeER6QU5CZ05\
QkFNTUJsUmxjM1JEUVRCWk1CTUdCeXFHU000OUFnRUdDQ3FHU000OUF3RUh\
MElBQk9rdmtUSHU4UWxUM0ZISjFVYUk3K1dzSE9iMFVTM1NBTHRHNXd1S1F\
amlleDA2L1NjWTVQSmlidmdIVEIrRi9RVGpnZWxIR3kxWUtwd2NOTWNzU3l\
alJUQkRNQklHQTFVZEV3RUIvd1FJTUFZQkFmOENBUUV3RGdZRFZSMFBBUUg\
QkFRREFnSUVNQjBHQTFVZERnUVdCQlRvWklNelFkc0Qvai8rZ1gvN2NCSnV\
SC9YbWpBS0JnZ3Foa2pPUFFRREFnTkpBREJHQWlFQXR4UTMrSUxHQlBJdFN\
NGI5V1hoWE51aHFTUDZIK2IvTEMvZlZZRGpRNm9DSVFERzJ1UkNIbFZxM3l\
QjU4VFhNVWJ6SDgrT2xoV1V2T2xSRDNWRXFEZGNRdz09Il19.eyJpZXRmLX\
vdWNoZXItcmVxdWVzdDp2b3VjaGVyIjp7InNlcmlhbC1udW1iZXIiOiIwMT\
zNDU2Nzg5Iiwibm9uY2UiOiJlRHMrKy9GdURIR1VuUnhOM0UxNENRPT0iLC\
wcmlvci1zaWduZWQtdm91Y2hlci1yZXF1ZXN0IjoiZXlKaGJHY2lPaUFpUl\
NeU5UWWlMQ0FpZURWaklqb2dXeUpOU1VsQ01tcERRMEZaUTJkQmQwbENRV2\
KUjBGWFpXZGtZMU5NVFVGdlIwTkRjVWRUVFRRNVFrRk5RMDFFTUhoRGVrRk\
RbWRPVmtKQldWUkJhMFpTVFZKVmQwVjNXVVJXVVZGTFJFRjRTMkZYTlc1VG\
XeDFXakJPZG1OdVFYaEdla0ZXUW1kT1ZrSkJUVTFFYTNCd1ltMWtTMkZYTl\
1V1IxWjZaRVZPUWsxRFFWaEVWRVUwVFZSSmVFMXFRWHBOYW1jeFRWWnZXVV\
2YXpWUFZHdDRUV3BOZUUxcVRURlBWRlUxVjJwQ1UwMVJjM2REVVZsRVZsRl\
SMFYzU2tKVlZFVldUVUpOUjBFeFZVVkRaM2ROVTIxc2RWb3djSEJpYldSRV\
qTktkMDFTVFhkRlVWbEVWbEZSUmtWM2IzZE5WRWw2VGtSVk1rNTZaelZOVW\
OM1JsRlpSRlpSVVVSRVFUVkxZVmMxYmxOdGJIVmFNRkpzWkcxc2FscFVRbH\
OUWsxSFFubHhSMU5OTkRsQlowVkhRME54UjFOTk5EbEJkMFZJUVRCSlFVSk\
Wa2RIT0ZvMWNHcG1OV3BZYm5seVZYSlllVm94YTFCbmNVSmxNMDVZZFRGa1\
FRkVaU3R5TDNZMlNucEpTR3d6TlRWSloyTklRek5oZUhCcFluRktUUzlpVj\
KaFJYbHFjV05EU21vMGFrcHJiM2REZFdwV1ZFSlVUVU4zUjBOVGMwZEJVVk\
DWjNVMVUwRm5VV1pFUWpGMFdWaE9hRXhZVW14ak0xRjFZekpzYkdKWFZuVm\
lVEZwWkVNMWRWcFlVVFpQVkZFd1RYcEJWRUpuVGxaSVUxVkZSRVJCUzBKbl\
zSkNaMFZHUWxGalJFRnFRVTlDWjA1V1NGRTRRa0ZtT0VWQ1FVMURRalJCZD\
ObldVbExiMXBKZW1vd1JVRjNTVVJUUVVGM1VsRkpaMWQwVUhwSlNWaFpNbW\
0VWxoS2RFVjRTMFZvYUZwa1lUUllLMFZ3YkZwdmJVVkpNbnBCTUdSemFtOU\
```

```
TVkZETTBwd1VXMVNXRTFIYmk5d05FSjFPV2w2YVdrNU1tVmpiRlI0TkM5UE\
ISnNiVGROZVV4eGEyaGtRVDA5SWwxOS5leUpwWlhSbUxYWnZkV05vWlhJdG\
tVnhkV1Z6ZERwMmIzVmphR1Z5SWpvZ2V5SmpjbVZoZEdWa0xXOXVJam9nSW\
Jd01qQXRNVEF0TWpKVU1ESTZNemM2TXprdU1EQXdXaUlzSUNKdWIyNWpaU0\
2SUNKbFJITXJLeTlHZFVSSVIxVnVVbmhPTTBVeE5FTlJQVDBpTENBaWMyVn\
hV0ZzTFc1MWJXSmxjaUk2SUNJd01USXpORFUyTnpnNUluMTkuVmo5cHlvND\
LREVxMGU1dG9rd0hwTmhWTTB1VWtMQ2F0d05ReGZzQ0tIOEdSUTJpVFQyZn\
EMzlrNDBNLTdTLXZoZURISHVCSEZTV2I1MDJFUHdrZEEiLCJjcmVhdGVkLW\
uIjoiMjAyMC0xMC0yMlQwMjozNzozOS4yMzVaIn19.S3BRYIKHbsqwQEZsB\
J1COIVAxO2NPEc5oo_BnXK_JkQfStTIeHFCALdv5MzYdTu9myJO1muaSFEI\
_NFMSFjA
```

<CODE ENDS>

It contains the following three parts:

Header:

<CODE BEGINS> file "parboiled_voucher_request_01-header.b64"

```
{
  "alg": "ES256",
  "x5c": [
    "MIIBozCCAUqgAwIBAgIGAW0eLuIFMAoGCCqGSM49BAMCMDUxEzARBg\
VBAoMCk15QnVzaW5lc3MxDTALBgNVBAcMBFNpdGUxDzANBgNVBAMMBlRlc3\
DQTAeFw0xOTA5MTEwMjM3MzJaFw0yOTA5MTEwMjM3MzJaMFQxEzARBgNVBA\
MCk15QnVzaW5lc3MxDTALBgNVBAcMBFNpdGUxLjAsBgNVBAMMJVJlZ2lzdH\
hciBWb3VjaGVyIFJlcXVlc3QgU2lnbmluZyBLZXkwWTATBgcqhkjOPQIBBg\
qhkjOPQMBBwNCAAT6xVvAvqTz1ZUiuNWhXpQskaPy7AHHQLwXiJ0iELt6uN\
anAN0QnWMYO/0CDEjIkBQobw8YKqjtxJHVSGTj9KOoycwJTATBgNVHSUEDD\
KBggrBgEFBQcDHDAOBgNVHQ8BAf8EBAMCB4AwCgYIKoZIzj0EAwIDRwAwRA\
gYr2LfqoaCKDF4RAcMmJi+NCZqdSiuVugISA7OhKRq3YCIDxnPMMnpXAMTr\
JuPWyceER11PxHOn+0CpSHi2qgpWX",
    "MIIBpDCCAUmgAwIBAgIGAW0eLuH+MAoGCCqGSM49BAMCMDUxEzARBg\
VBAoMCk15QnVzaW5lc3MxDTALBgNVBAcMBFNpdGUxDzANBgNVBAMMBlRlc3\
DQTAeFw0xOTA5MTEwMjM3MzJaFw0yOTA5MTEwMjM3MzJaMDUxEzARBgNVBA\
MCk15QnVzaW5lc3MxDTALBgNVBAcMBFNpdGUxDzANBgNVBAMMBlRlc3RDQT\
ZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABOkvkTHu8QlT3FHJ1UaI7+WsHO\
0US3SALtG5wuKQDjiex06/ScY5PJibvgHTB+F/QTjgelHGy1YKpwcNMcsSy\
jRTBDMBIGA1UdEwEB/wQIMAYBAf8CAQEwDgYDVR0PAQH/BAQDAgIEMB0GA1\
dDgQWBBToZIMzQdsD/j/+gX/7cBJucH/XmjAKBggqhkjOPQQDAgNJADBGAi\
AtxQ3+ILGBPItSh4b9WXhXNuhqSP6H+b/LC/fVYDjQ6oCIQDG2uRCHlVq3y\
B58TXMUbzH8+OlhWUvOlRD3VEqDdcQw=="
  ]
}
```

<CODE ENDS>

Payload:

<CODE BEGINS> file "parboiled_voucher_request_01-payload.b64"

```
{
  "ietf-voucher-request:voucher": {
    "serial-number": "0123456789",
    "nonce": "eDs++/FuDHGUnRxN3E14CQ==",
    "prior-signed-voucher-request": "eyJhbGciOiAiRVMyNTYiLC\
ieDVjIjogWyJNSUlCMmpDQ0FZQ2dBd0lCQWdJR0FXZWdkY1NMTUFvR0NDcU\
TTTQ5QkFNQ01EMHhDekFKQmdOVkJBWVRBa0ZSTVJVd0V3WURWUVFLREF4S2\
XNW5TbWx1WjBOdmNuQXhGekFWQmdOVkJBTU1Ea3BwYm1kS2FXNW5WR1Z6ZE\
OQk1DQVhEVEU0TVRJeE1qQXpNamcxTVZvWUR6azVPVGt4TWpNeE1qTTFPVF\
1V2pCU01Rc3dDUVlEVlFRR0V3SkJVVEVWTUJNR0ExVUVDZ3dNU21sdVowcH\
ibWREYjNKd01STXdFUVlEVlFRRkV3b3dNVEl6TkRVMk56ZzVNUmN3RlFZRF\
RUUREQTVLYVc1blNtbHVaMFJsZG1salpUQlpNQk1HQnlxR1NNNDlBZ0VHQ0\
xR1NNNDlBd0VIQTBJQUJNVkdHOFo1cGpmNWpYbnlyVXJYeVoxa1BncUJlM0\
YdTFkVEFEZStyL3Y2SnpJSGwzNTVJZ2NIQzNheHBpYnFKTS9iV1JhRXlqcW\
DSmo0akprb3dDdWpWVEJUTUN3R0NTc0dBUVFCZ3U1U0FnUWZEQjF0WVhOaE\
YUmxjM1F1YzJsbGJXVnVjeTFpZEM1dVpYUTZPVFEwTXpBVEJnTlZIU1VFRE\
BS0JnZ3JCZ0VGQlFjREFqQU9CZ05WSFE4QkFmOEVCQU1DQjRBd0NnWUlLb1\
JemowRUF3SURTQUF3UlFJZ1d0UHpJSVhZMml4UlhKdEV4S0VoaFpkYTRYK0\
wbFpvbUVJMnpBMGRzam9DSVFDM0pwUW1SWE1Hbi9wNEJ1OWl6aWk5MmVjbF\
4NC9PNHJsbTdNeUxxa2hkQT09Il19.eyJpZXRmLXZvdWNoZXItcmVxdWVzd\
p2b3VjaGVyIjogeyJjcmVhdGVkLW9uIjogIjIwMjAtMTAtMjJUMDI6Mzc6M\
kuMDAwWiIsICJub25jZSI6ICJlRHMrKy9GdURIR1VuUnhOM0UxNENRPT0iL\
Aic2VyaWFsLW51bWJlciI6ICIwMTIzNDU2Nzg5In19.Vj9pyo43KDEq0e5t\
kwHpNhVM0uUkLCatwNQxfsCKH8GRQ2iTT2fqD39k40M-7S-vheDHHuBHFSW\
502EPwkdA",
    "created-on": "2020-10-22T02:37:39.235Z"
  }
}
```

<CODE ENDS>

Signature:

<CODE BEGINS> file "parboiled_voucher_request_01-signature.b64"

```
S3BRYIKHbsqwQEZsBgJ1COIVAxO2NPEc5oo_BnXK_JkQfStTIeHFCALdv5M\
YdTu9myJO1muaSFEIu_NFMSFjA
```

<CODE ENDS>

### A.3. Example Voucher Result (from MASA to Pledge, via Registrar)

The following is an example voucher sent from the Registrar to the MASA. This example is from the Siemens reference MASA system.

<CODE BEGINS> file "voucher_01.b64"

```
eyJhbGciOiJFUzI1NiIsIng1YyI6WyJNSUlCa3pDQ0FUaWdBd0lCQWdJR0F\
RkJqQ2tZTUFvR0NDcUdTTTQ5QkFNQ01EMHhDekFKQmdOVkJBWVRBa0ZSTVJ\
d0V3WURWUVFLREF4S2FXNW5TbWx1WjBOdmNuQXhGekFWQmdOVkJBTU1Ea3B\
Ym1kS2FXNW5WR1Z6ZEVOQk1CNFhEVEU0TURFeU9URXdOVEkwTUZvWERUSTR\
REV5T1RFd05USTBNRm93VHpFTE1Ba0dBMVVFQmhNQ1FWRXhGVEFUQmdOVkJ\
b01ERXBwYm1kS2FXNW5RMjl5Y0RFcE1DY0dBMVVFQXd3Z1NtbHVaMHBwYm1\
RGIzSndJRlp2ZFdOb1pYSWdVMmxuYm1sdVp5QkxaWGt3V1RBVEJnY3Foa2p\
UFFJQkJnZ3Foa2pPUFFNQkJ3TkNBQVNDNmJlTEFtZXExVnc2aVFyUnM4UjB\
Vys0YjFHV3lkbVdzMkdBTUZXd2JpdGYybklYSDNPcUhLVnU4czJSdmlCR05\
dk9LR0JISHRCZGlGRVpadmI3b3hJd0VEQU9CZ05WSFE4QkFmOEVCQU1DQjR\
d0NnWUlLb1pJemowRUF3SURTUUF3UmdJaEFJNFBZYnh0c3NIUDJWSHgvdHp\
b1EvU3N5ZEwzMERRSU5FdGNOOW1DVFhQQWlFQXZJYjNvK0ZPM0JUbmNMRnN\
SlpSQWtkN3pPdXNuLy9aS09hRUtic1ZEaVU9Il19.eyJpZXRmLXZvdWNoZX\
6dm91Y2hlciI6eyJhc3NlcnRpb24iOiJsb2dnZWQiLCJzZXJpYWwtbnVtYm\
yIjoiMDEyMzQ1Njc4OSIsIm5vbmNlIjoiZURzKysvRnVESEdVblJ4TjNFMT\
DUT09IiwiY3JlYXRlZC1vbiI6IjIwMjAtMTAtMjJUMDI6Mzc6MzkuOTIxWi\
sInBpbm5lZC1kb21haW4tY2VydCI6Ik1JSUJwRENDQVVtZ0F3SUJBZ0lHQV\
wZUx1SCtNQW9HQ0NxR1NNNDlCQU1DTURVeEV6QVJCZ05WQkFvTUNrMTVRbl\
6YVc1bGMzTXhEVEFMQmdOVkJBY01CRk5wZEdVeER6QU5CZ05WQkFNTUJsUm\
jM1JEUVRBZUZ3MHhPVEE1TVRFd01qTTNNekphRncweU9UQTVNVEV3TWpNM0\
6SmFNRFV4RXpBUkJnTlZCQW9NQ2sxNVFuVnphVzVsYzNNeERUQUxCZ05WQk\
jTUJGTnBkR1V4RHpBTkJnTlZCQU1NQmxSbGMzUkRRVEJaTUJNR0J5cUdTTT\
5QWdFR0NDcUdTTTQ5QXdFSEEwSUFCT2t2a1RIdThRbFQzRkhKMVVhSTcrV3\
IT2IwVVMzU0FMdEc1d3VLUURqaWV4MDYvU2NZNVBKaWJ2Z0hUQitGL1FUam\
lbEhHeTFZS3B3Y05NY3NTeWFqUlRCRE1CSUdBMVVkRXdFQi93UUlNQVlCQW\
4Q0FRRXdEZ1lEVlIwUEFRSC9CQVFEQWdJRU1CMEdBMVVkRGdRV0JCVG9aSU\
6UWRzRC9qLytnWC83Y0JKdWNIL1htakFLQmdncWhrak9QUVFEQWdOSkFEQk\
BaUVBdHhRMytJTEdCUEl0U2g0YjlXWGhYTnVocVNQNkgrYi9MQy9mVllEal\
2b0NJUURHMnVSQ0hsVnEzeWhCNThUWE1VYnpIOCtPbGhXVXZPbFJEM1ZFcU\
kY1F3PT0ifX0.u1iO_VB6xIhE8QuhKDGgCxkzsnR20IoL0p6qYKpYBDtgkR\
2ykDO_QFjk7W8P5ATW-CQnWlJ3ILSeiwMf9nI0g
```

<CODE ENDS>

It contains the following three parts:

Header:

<CODE BEGINS> file "voucher_01-header.b64"

```
{
  "alg": "ES256",
  "x5c": [
    "MIIBkzCCATigAwIBAgIGAWFBjCkYMAoGCCqGSM49BAMCMD0xCzAJBg\
VBAYTAkFRMRUwEwYDVQQKDAxKaW5nSmluZ0NvcnAxFzAVBgNVBAMMDkppbm\
KaW5nVGVzdENBMB4XDTE4MDEyOTEwNTI0MFoXDTI4MDEyOTEwNTI0MFowTz\
LMAkGA1UEBhMCQVExFTATBgNVBAoMDEppbmdKaW5nQ29ycDEpMCcGA1UEAw\
gSmluZ0ppbmdDb3JwIFZvdWNoZXIgU2lnbmluZyBLZXkwWTATBgcqhkjOPQ\
BBggqhkjOPQMBBwNCAASC6beLAmeq1Vw6iQrRs8R0ZW+4b1GWydmWs2GAMF\
wbitf2nIXH3OqHKVu8s2RviBGNivOKGBHHtBdiFEZZvb7oxIwEDAOBgNVHQ\
BAf8EBAMCB4AwCgYIKoZIzj0EAwIDSQAwRgIhAI4PYbxtssHP2VHx/tzUoQ\
SsydL30DQINEtcN9mCTXPAiEAvIb3o+FO3BTncLFsaJZRAkd7zOusn//ZKO\
EKbsVDiU="
  ]
}
```

<CODE ENDS>

Payload:

<CODE BEGINS> file "voucher_01-payload.b64"

```
{
  "ietf-voucher:voucher": {
    "assertion": "logged",
    "serial-number": "0123456789",
    "nonce": "eDs++/FuDHGUnRxN3E14CQ==",
    "created-on": "2020-10-22T02:37:39.921Z",
    "pinned-domain-cert": "MIIBpDCCAUmgAwIBAgIGAW0eLuH+MAoG\
CqGSM49BAMCMDUxEzARBgNVBAoMCk15QnVzaW5lc3MxDTALBgNVBAcMBFNp\
GUxDzANBgNVBAMMBlRlc3RDQTAeFw0xOTA5MTEwMjM3MzJaFw0yOTA5MTEw\
jM3MzJaMDUxEzARBgNVBAoMCk15QnVzaW5lc3MxDTALBgNVBAcMBFNpdGUx\
zANBgNVBAMMBlRlc3RDQTBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABOkv\
THu8QlT3FHJ1UaI7+WsHOb0US3SALtG5wuKQDjiex06/ScY5PJibvgHTB+F\
QTjgelHGy1YKpwcNMcsSyajRTBDMBIGA1UdEwEB/wQIMAYBAf8CAQEwDgYD\
R0PAQH/BAQDAgIEMB0GA1UdDgQWBBToZIMzQdsD/j/+gX/7cBJucH/XmjAK\
ggqhkjOPQQDAgNJADBGAiEAtxQ3+ILGBPItSh4b9WXhXNuhqSP6H+b/LC/f\
YDjQ6oCIQDG2uRCHlVq3yhB58TXMUbzH8+OlhWUvOlRD3VEqDdcQw=="
  }
}
```

<CODE ENDS>

Signature:

```
<CODE BEGINS> file "voucher_01-signature.b64"

u1iO_VB6xIhE8QuhKDGgCxkzsnR20IoL0p6qYKpYBDtgkRT2ykDO_QFjk7W\
P5ATW-CQnWlJ3ILSeiwMf9nI0g

<CODE ENDS>
```

## Authors' Addresses


Michael Richardson
Sandelman Software Works

Email: mcr+ietf@sandelman.ca

Thomas Werner
Siemens

Email: thomas-werner@siemens.com