Workgroup: anima Working Group
Internet-Draft:
draft-ietf-anima-jws-voucher-04
Updates: RFC8366 (if approved)
Published: 11 July 2022
Intended Status: Standards Track
Expires: 12 January 2023
Authors: T. Werner M. Richardson
Siemens AG Sandelman Software Works

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 12 January 2023.

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 from a manufacturer to an owner. That document defines the base YANG module and the serialization to JSON [RFC8259] with a CMS signature according to [RFC5652]. The resulting Voucher artifact has the media type "application/voucher-cms+json".

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 JSON Web Signature (JWS) [RFC7515]. The encoding specified in this document is used by [I-D.ietf-anima-brski-prm] and may be preferred for use cases requiring signed JSON objects.

This document does not extend the YANG definition of [RFC8366].

With the availability of different encoded vouchers, it is up to an industry specific application statement to indicate/decide which voucher signature format is to be used. There is no provision across the different voucher signature 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 artifact.

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. Voucher Artifact with JSON Web Signature

The voucher [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.

A JWS JSON Serialization Overview is given by The following serializations are defined:[RFC7515] in section 3.2 and section 7 provides more details.

1. "JWS Compact Serialization", [RFC7515] section 7.1

2. "JWS JSON Serialization" in, [RFC7515] section 7.2

   - "General JWS JSON Serialization Syntax", [RFC7515] section 7.2.1

   - "Flattened JWS JSON Serialization Syntax", [RFC7515] section 7.2.2

This document makes use of the "General JWS JSON Serialization Syntax" to support multi signatures.

[RFC Editor: please delete] /* TODO: ... */

[RFC Editor: please delete] /*
TODO: ...
*/

There are a number of attributes. They are:

3.1. Unprotected Header

[RFC Editor: please delete] /* TODO: ... */

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.

3.3. Voucher Representation in General JWS JSON Serialization Syntax

```
{
  "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=="
    }
  ]
}
```

Figure 1: Voucher Representation in General JWS JSON Serialization Syntax

4. Privacy Considerations

The Voucher Request reveals the IDevID of the component (Pledge) that is on-boarding.

This request occurs over HTTP-over-TLS, 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-jws+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.

*Updated references "I-D.ietf-anima-brski-async-enroll" switched to "I-D.ietf-anima-brski-prm"

*Switch from "JWS Compact Serialization" to "General JWS JSON Serialization", as focus is now on "General JWS JSON Serialization"

*Include Voucher representation in "General JWS JSON Serialization" syntax

*Include examples A1, A2, A3 using "General JWS JSON Serialization"

*Added optional "typ": "voucher-jws+json" header parameter to JWS objects

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.ietf-anima-brski-prm] Fries, S., Werner, T., Lear, E., and M. C. Richardson, "BRSKI with Pledge in Responder Mode (BRSKI-PRM)", Work in Progress, Internet-Draft, draft-ietf-anima-brski-prm-04, 8 July 2022, <https://

www.ietf.org/archive/id/draft-ietf-anima-brski-prm-04.txt>.

[I-D.ietf-anima-constrained-voucher] Richardson, M., Stok, P. V. D., Kampanakis, P., and E. Dijk, "Constrained Bootstrapping Remote Secure Key Infrastructure (BRSKI)", Work in Progress, Internet-Draft, draft-ietf-anima-constrained-voucher-17, 7 April 2022, <https://www.ietf.org/archive/id/draft-ietf-anima-constrained-voucher-17.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>.

[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 Pledge Voucher Request - PVR (from Pledge to Registrar)

The following is an example request sent from a Pledge to the Registrar, in "General JWS JSON Serialization".

```
{
   "payload":
     "eyJpZXRmLXZvdWNoZXItcmVxdWVzdDp2b3VjaGVyIjp7InNlcmlhbC1
     udW1iZXIiOiIwMTIzNDU2Nzg5Iiwibm9uY2UiOiI2R3RuK1pRS04ySHF
     ERlZrQkV4WkxRPT0iLCJjcmVhdGVkLW9uIjoiMjAyMi0wNy0wOFQwODo
     0MDo0Mi44MjBaIiwicHJveGltaXR5LXJlZ2lzdHJhci1jZXJ0IjoiTUl
     JQjRqQ0NBWWlnQXdJQkFnSUdBWFk3MmJiWk1Bb0dDQ3FHU000OUJBTUN
     NRFV4RXpBUkJnTlZCQW9NQ2sxNVFuVnphVzVsYzNNeERUQUxCZ05WQkF
     jTUJGTnBkR1V4RHpBTkJnTlZCQU1NQmxSbGMzUkRRVEFlRncweU1ERXl
     NRGN3TmpFNE1USmFGdzB6TURFeU1EY3dOakU0TVRKYU1ENHhFekFSQmd
     OVkJBb01DazE1UW5WemFXNWxjM014RFRBTEJnTlZCQWNNQkZOcGRHVXh
     HREFXQmdOVkJBTU1EMFJ2YldGcGJsSmxaMmx6ZEhKaGNqQlpNQk1HQnl
     xR1NNNDlBZ0VHQ0NxR1NNNDlBd0VIQTBJQUJCazE2Sy9pNzlvUmtLNVl
     iZVBnOFVTUjgvdXMxZFBVaVpITXRva1NkcUtXNWZuV3NCZCtxUkw3V1J
     mZmVXa3lnZWJvSmZJbGx1cmNpMjV3bmhpT1ZDR2plekI1TUIwR0ExVWR
     KUVFXTUJRR0NDc0dBUVVGQndNQkJnZ3JCZ0VGQlFjREhEQU9CZ05WSFE
     4QkFmOEVCQU1DQjRBd1NBWURWUjBSQkVFd1A0SWRjbVZuYVhOMGNtRnl
     MWFJsYzNRdWMybGxiV1Z1Y3kxaWRDNXVaWFNDSG5KbFoybHpkSEpoY2k
     xMFpYTjBOaTV6YVdWdFpXNXpMV0owTG01bGREQUtCZ2dxaGtqT1BRUUR
     BZ05JQURCRkFpQnhsZEJoWnEwRXY1SkwyUHJXQ3R5UzZoRFlXMXlDTy9
     SYXVicEM3TWFJRGdJaEFMU0piZ0xuZ2hiYkFnMGRjV0ZVVm8vZ0dOMC9
     qd3pKWjBTbDJoNHhJWGsxIn19",
   "signatures": [
      {
         "protected":
           "eyJ4NWMiOlsiTUlJQitUQ0NBYUNnQXdJQkFnSUdBWG5WanNVNU1Bb0d
           DQ3FHU000OUJBTUNNRDB4Q3pBSkJnTlZCQVlUQWtGUk1SVXdFd1lEVlF
           RS0RBeEthVzVuU21sdVowTnZjbkF4RnpBVkJnTlZCQU1NRGtwcGJtZEt
           hVzVuVkdWemRFTkJNQ0FYRFRJeE1EWXdOREExTkRZeE5Gb1lEems1T1R
           reE1qTXhNak0xT1RVNVdqQlNNUXN3Q1FZRFZRUUdFd0pCVVRFVk1CTUd
           BMVVFQ2d3TVNtbHVaMHBwYm1kRGIzSndNUk13RVFZRFZRUUZFd293TVR
           Jek5EVTJOemc1TVJjd0ZRWURWUVFEREE1S2FXNW5TbWx1WjBSbGRtbGp
           aVEJaTUJNR0J5cUdTTTQ5QWdFR0NDcUdTTTQ5QXdFSEEwSUFCQzc5bGl
           hUmNCalpjRUVYdzdyVWVhdnRHSkF1SDRwazRJNDJ2YUJNc1UxMWlMREN
           DTGtWaHRVVjIxbXZhS0N2TXgyWStTTWdROGZmd0wyM3ozVElWQldqZFR
           Cek1Dc0dDQ3NHQVFVRkJ3RWdCQjhXSFcxaGMyRXRkR1Z6ZEM1emFXVnR
           aVzV6TFdKMExtNWxkRG81TkRRek1COEdBMVVkSXdRWU1CYUFGRlFMak5
           6UFwvU1wva291alF3amc1RTVmdndjWWJNQk1HQTFVZEpRUU1NQW9HQ0N
           zR0FRVUZCd01DTUE0R0ExVWREd0VCXC93UUVBd0lIZ0RBS0JnZ3Foa2p
           PUFFRREFnTkhBREJFQWlCdTN3UkJMc0pNUDVzTTA3MEgrVUZyeU5VNmd
           LekxPUmNGeVJST2xxcUhpZ0lnWENtSkxUekVsdkQycG9LNmR4NmwxXC9
           1eW1UbmJRRERmSmxhdHVYMlJvT0U9Il0sInR5cCI6InZvdWNoZXItand
           zK2pzb24iLCJhbGciOiJFUzI1NiJ9",
         "signature":
           "abVg4TDGzSTjVHkQlNeIW3ABu5ZXdMl1cEqwcIAlHFW4BrlGbO-DRTK
           fyCOGxSW49-ktJcrVlYgKqC4xmZoy0Q"
      }
   ]
}
```

Figure 2: Example Pledge Voucher Request - PVR

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

The term parboiled refers to food which is partially cooked. In [BRSKI], the term refers to a Pledge voucher-request (PVR) 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 Registrar voucher-request (RVR) sent from the Registrar to the MASA, in "General JWS JSON Serialization". Note that the previous PVR can be seen in the payload as "prior-signed-voucher-request".

```
{
   "payload":
     "eyJpZXRmLXZvdWNoZXItcmVxdWVzdDp2b3VjaGVyIjp7InNlcmlhbC1
     udW1iZXIiOiIwMTIzNDU2Nzg5IiwiaWRldmlkLWlzc3VlciI6IkJCZ3d
     Gb0FVVkF1TTNNLzlMK1NpNk5EQ09Ea1RsKy9CeGhzPSIsIm5vbmNlIjo
     iNkd0bitaUUtOMkhxREZWa0JFeFpMUT09IiwicHJpb3Itc2lnbmVkLXZ
     vdWNoZXItcmVxdWVzdCI6ImV5SndZWGxzYjJGa0lqb2laWGxLY0ZwWVV
     tMU1XRnAyWkZkT2IxcFlTWFJqYlZaNFpGZFdlbVJFY0RKaU0xWnFZVWR
     XZVVscWNEZEpiazVzWTIxc2FHSkRNWFZrVnpGcFdsaEphVTlwU1hkTlZ
     FbDZUa1JWTWs1Nlp6VkphWGRwWW0wNWRWa3lWV2xQYVVreVVqTlNkVXN
     4Y0ZKVE1EUjVVMGhHUlZKc1duSlJhMVkwVjJ0NFVsQlVNR2xNUTBwcVk
     yMVdhR1JIVm10TVZ6bDFTV3B2YVUxcVFYbE5hVEIzVG5rd2QwOUdVWGR
     QUkc4d1RVUnZNRTFwTkRSTmFrSmhTV2wzYVdOSVNuWmxSMngwWVZoU05
     VeFlTbXhhTW14NlpFaEthR05wTVdwYVdFb3dTV3B2YVZSVmJFcFJhbEp
     4VVRCT1FsZFhiRzVSV0dSS1VXdEdibE5WWkVKWFJtc3pUVzFLYVZkck1
     VSmlNR1JFVVROR1NGVXdNREJQVlVwQ1ZGVk9UbEpHVmpSU1dIQkNWV3R
     LYmxSc1drTlJWemxPVVRKemVFNVdSblZXYm5Cb1ZucFdjMWw2VGs1bFJ
     WSlZVVlY0UTFvd05WZFJhMFpxVkZWS1IxUnVRbXRTTVZZMFVraHdRbFJ
     yU201VWJGcERVVlV4VGxGdGVGTmlSMDE2Vld0U1VsWkZSbXhTYm1OM1p
     WVXhSVkpZYkU1U1IwNHpWRzF3Ums1Rk1WVlRiVVpIWkhwQ05sUlZVa1p
     sVlRGRldUTmtUMkZyVlRCVVZsSkxXVlV4UlU1SWFFWmxhMFpUVVcxa1Q
     xWnJTa0ppTURGRVlYcEZNVlZYTlZkbGJVWllUbGQ0YWswd01UUlNSbEp
     DVkVWS2JsUnNXa05SVjA1T1VXdGFUMk5IVWtoV1dHaElVa1ZHV0ZGdFp
     FOVdhMHBDVkZVeFJVMUdTakpaYkdSSFkwZEtjMU50ZUdGTmJYZzJXa1Z
     vUzJGSFRuRlJiSEJPVVdzeFNGRnViSGhTTVU1T1RrUnNRbG93VmtoUk1
     FNTRVakZPVGs1RWJFSmtNRlpKVVZSQ1NsRlZTa05oZWtVeVUzazVjRTU
     2YkhaVmJYUk1UbFpzYVZwV1FtNVBSbFpVVldwbmRtUllUWGhhUmtKV1l
     WWndTVlJZVW5aaE1VNXJZMVYwV0U1WFduVldNMDVEV2tOMGVGVnJkek5
     XTVVwdFdtMVdXR0V6Ykc1YVYwcDJVMjFhU21KSGVERmpiVTV3VFdwV00
     ySnRhSEJVTVZwRVVqSndiR1ZyU1RGVVZVbDNVakJGZUZaWFVrdFZWa1p
     ZVkZWS1VsSXdUa1JqTUdSQ1ZWWldSMUZ1WkU1UmEwcHVXak5LUTFvd1Z
     rZFJiRVpxVWtWb1JWRlZPVU5hTURWWFUwWkZORkZyUm0xUFJWWkRVVlV
     4UkZGcVVrSmtNVTVDVjFWU1YxVnFRbE5SYTFaR1pERkJNRk5YVW1waVZ
     scDFXVlpvVDAxSFRuUlNibXhOVjBaS2MxbDZUbEprVjAxNVlrZDRhVll
     4V2pGWk0ydDRZVmRTUkU1WVZtRlhSazVFVTBjMVMySkdiM2xpU0hCclU
     wVndiMWt5YTNoTlJuQlpWR3BDVDJGVVZqWlpWbVJYWkVad1dFNVljRTF
     XTUc5M1ZFY3dNV0pIVWtWUlZYUkRXakprZUdGSGRIRlVNVUpTVlZWU1F
     sb3dOVXBSVlZKRFVtdEdjRkZ1YUhOYVJVcHZWMjVGZDFKWVdURlRhM2Q
     1VlVoS1dGRXpValZWZWxwdlVrWnNXRTFZYkVSVWVUbFRXVmhXYVdORlR
     UTlVWMFpLVWtka1NtRkZSazFWTUhCcFdqQjRkVm95YUdsWmEwWnVUVWR
     TYWxZd1dsWldiVGgyV2pCa1QwMURPWEZrTTNCTFYycENWR0pFU205T1N
     HaEtWMGR6ZUVsdU1Ua2lMQ0p6YVdkdVlYUjFjbVZ6SWpwYmV5SndjbTk
     wWldOMFpXUWlPaUpsZVVvMFRsZE5hVTlzYzJsVVZXeEtVV2wwVlZFd1R
     rSlpWVTV1VVZoa1NsRnJSbTVUVldSQ1YwYzFWMkZ1VGxaT1ZURkNZakJ
     rUkZFelJraFZNREF3VDFWS1FsUlZUazVTUkVJMFVUTndRbE5yU201VWJ
     GcERVVlpzVlZGWGRFZFZhekZUVmxoa1JtUXhiRVZXYkVaU1V6QlNRbVZ
     GZEdoV2VsWjFWVEl4YzJSV2IzZFVibHBxWW10R05GSnVjRUpXYTBwdVZ
     HeGFRMUZWTVU1U1IzUjNZMGRLZEZwRmRHaFdlbFoxVm10a1YyVnRVa1p
     VYTBwT1VUQkdXVkpHVWtwbFJURkZWMWhrVDFKRlJYaFVhMUphWlVVMVI
```

```
  ySXhiRVZsYlhNeFZERlNjbVZGTVhGVVdHaE9ZV3N3ZUZReFVsWk9WbVJ
  4VVd4T1RsVllUak5STVVaYVVrWmFVbFZWWkVaa01IQkRWbFpTUmxack1
  VTlVWV1JDVFZaV1JsRXlaRE5VVms1MFlraFdZVTFJUW5kWmJURnJVa2R
  KZWxOdVpFNVZhekV6VWxaR1dsSkdXbEpWVlZwR1pESTVNMVJXVWtwbGF
  6VkZWbFJLVDJWdFl6RlVWa3BxWkRCYVVsZFZVbGRWVmtaRlVrVkZNVk1
  5UmxoT1Z6VlVZbGQ0TVZkcVFsTmlSMUowWWtkd1lWWkZTbUZVVlVwT1V
  qQktOV05WWkZSVVZGRTFVVmRrUmxJd1RrUmpWV1JVVkZSUk5WRllaRVp
  UUlVWM1UxVkdRMUY2WXpWaVIyeG9WVzFPUTJGc2NHcFNWVlpaWkhwa2V
  WWlhWbWhrYmxKSVUydEdNVk5FVW5kaGVsSktUa1JLTWxsVlNrNWpNVlY
  0VFZkc1RWSkZUa1JVUjNSWFlVaFNWbFpxU1hoaVdGcG9VekJPTWxSWVo
  zbFhVM1JVVkZka1VrOUhXbTFrTUhkNVRUTnZlbFpGYkZkUmJHUnhXa1p
  TUTJWck1VUmpNR1JFVVROT1NGRldSbFpTYTBvelVsZGtRMUZxYUZoVFJ
  tTjRZVWROZVZKWVVtdFNNVm8yV2tWTk1XVnRSbGhXYmxKaFZucFdObFJ
  HWkV0TlJYaDBUbGQ0YTFKSE9ERlVhMUpTWldzeFEwOUZaRUpOVmxaclU
  xaGtVbGRWTVVOWlZVWkhVbXhHVFdGck5UWlZSbmQyVlRGM2RtRXlPVEZ
  oYkVZellXMWpNVkpVVm0xa2JtUnFWMWRLVGxGck1VaFJWRVpXV2tWd1V
  sVlZNVTVSVnpsSVVUQk9lbEl3UmxKV1ZWcERaREF4UkZSVlJUQlNNRVY
  0VmxkU1JXUXdWa05ZUXprelZWVldRbVF3YkVsYU1GSkNVekJLYmxvelJ
  tOWhNbkJRVlVaR1VsSkZSbTVVYTJoQ1VrVktSbEZYYkVOa1ZFNHpWV3R
  LVFdNd2NFNVZSRlo2VkZSQk0wMUZaM0pXVlZwNVpWVTFWazV0WkV4bGE
  zaFFWVzFPUjJWV1NsTlVNbmg0WTFWb2NGb3diRzVYUlU1MFUydDRWV1Z
  yVm5Oa2ExRjVZMGM1VEU1dFVqUk9iWGQ0V0VNNU1XVlhNVlZpYlVwU1V
  rVlNiVk50ZUdoa1NGWlpUV3hLZGxRd1ZUbEpiREJ6U1c1U05XTkRTVFp
  KYmxwMlpGZE9iMXBZU1hSaGJtUjZTekp3ZW1JeU5HbE1RMHBvWWtkamF
  VOXBTa1pWZWtreFRtbEtPU0lzSW5OcFoyNWhkSFZ5WlNJNkltRmlWbWM
  wVkVSSGVsTlVhbFpJYTFGc1RtVkpWek5CUW5VMVdsaGtUV3d4WTBWeGQ
  yTkpRV3hJUmxjMFFuSnNSMkpQTFVSU1ZFdG1lVU5QUjNoVFZ6UTVMV3Q
  wU21OeVZteFpaMHR4UXpSNGJWcHZlVEJSSW4xZGZRPT0iLCJjcmVhdGV
  kLW9uIjoiMjAyMi0wNy0wOFQwODo0MDo0Mi44NDhaIn19",
"signatures": [
   {
      "protected":
        "eyJ4NWMiOlsiTUlJQm96Q0NBVXFnQXdJQkFnSUdBVzBlTHVJRk1Bb0d
        DQ3FHU000OUJBTUNNRFV4RXpBUkJnTlZCQW9NQ2sxNVFuVnphVzVsYzN
        NeERUQUxCZ05WQkFjTUJGTnBkR1V4RHpBTkJnTlZCQU1NQmxSbGMzUkR
        RVEFlRncweE9UQTVNVEV3TWpNM016SmFGdzB5T1RBNU1URXdNak0zTXp
        KYU1GUXhFekFSQmdOVkJBb01DazE1UW5WemFXNWxjM014RFRBTEJnTlZ
        CQWNNQkZOcGRHVXhMakFzQmdOVkJBTU1KVkpsWjJsemRISmhjaUJXYjN
        WamFHVnlJRkpsY1hWbGMzUWdVMmxuYm1sdVp5QkxaWGt3V1RBVEJnY3F
        oa2pPUFFJQkJnZ3Foa2pPUFFNQkJ3TkNBQVQ2eFZ2QXZxVHoxWlVpdU5
        XaFhwUXNrYVB5N0FISFFMd1hpSjBpRUx0NnVOUGFuQU4wUW5XTVlPXC8
        wQ0RFaklrQlFvYnc4WUtxanR4SkhWU0dUajlLT295Y3dKVEFUQmdOVkh
        TVUVEREFLQmdnckJnRUZCUWNESERBT0JnTlZIUThCQWY4RUJBTUNCNEF
        3Q2dZSUtvWkl6ajBFQXdJRFJ3QXdSQUlnWXIyTGZxb2FDS0RGNFJBY01
        tSmkrTkNacWRTaXVWdWdJU0E3T2hLUnEzWUNJRHhuUE1NbnBYQU1UclB
        KdVBXeWNlRVIxMVB4SE9uKzBDcFNIaTJxZ3BXWCIsIk1JSUJwRENDQVV
        tZ0F3SUJBZ0lHQVcwZUx1SCtNQW9HQ0NxR1NNNDlCQU1DTURVeEV6QVJ
        CZ05WQkFvTUNrMTVRblZ6YVc1bGMzTXhEVEFMQmdOVkJBY01CRk5wZEd
        VeER6QU5CZ05WQkFNTUJsUmxjM1JEUVRBZUZ3MHhPVEE1TVRFd01qTTN
```

```
          NekphRncweU9UQTVNVEV3TWpNM016SmFNRFV4RXpBUkJnTlZCQW9NQ2s
          xNVFuVnphVzVsYzNNeERUQUxCZ05WQkFjTUJGTnBkR1V4RHpBTkJnTlZ
          CQU1NQmxSbGMzUkRRVEJaTUJNR0J5cUdTTTQ5QWdFR0NDcUdTTTQ5QXd
          FSEEwSUFCT2t2a1RIdThRbFQzRkhKMVVhSTcrV3NIT2IwVVMzU0FMdEc
          1d3VLUURqaWV4MDZcL1NjWTVQSmlidmdIVEIrRlwvUVRqZ2VsSEd5MVl
          LcHdjTk1jc1N5YWpSVEJETUJJR0ExVWRFd0VCXC93UUlNQVlCQWY4Q0F
          RRXdEZ1lEVlIwUEFRSFwvQkFRREFnSUVNQjBHQTFVZERnUVdCQlRvWkl
          NelFkc0RcL2pcLytnWFwvN2NCSnVjSFwvWG1qQUtCZ2dxaGtqT1BRUUR
          BZ05KQURCR0FpRUF0eFEzK0lMR0JQSXRTaDRiOVdYaFhOdWhxU1A2SCt
          iXC9MQ1wvZlZZRGpRNm9DSVFERzJ1UkNIbFZxM3loQjU4VFhNVWJ6SDg
          rT2xoV1V2T2xSRDNWRXFEZGNRdz09Il0sInR5cCI6InZvdWNoZXItand
          zK2pzb24iLCJhbGciOiJFUzI1NiJ9",
        "signature":
          "0fzuqVdyhemWsu_HQeF-CmQwJeLp9IStNf-bWZwz6SojrEOR4aDq6VS
          tyG8eWXjGHNZiRyyLJo7RP1rKatuS2w"
      }
   ]
}
```

Figure 3: Example Parboiled Registrar Voucher Request - RVR

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

The following is an example voucher response from MASA to Pledge via Registrar, in "General JWS JSON Serialization".

```
{
    "payload":
      "eyJpZXRmLXZvdWNoZXI6dm91Y2hlciI6eyJhc3NlcnRpb24iOiJsb2
      dnZWQiLCJzZXJpYWwtbnVtYmVyIjoiMDEyMzQ1Njc4OSIsIm5vbmNlI
      joiZGRoSGQ4MlFpUGtzMDBTck1USTlEUT09IiwiY3JlYXRlZC1vbiI6
      IjIwMjItMDctMDdUMTc6NDc6MDEuODkwWiIsInBpbm5lZC1kb21haW4
      tY2VydCI6Ik1JSUJwRENDQVVtZ0F3SUJBZ0lHQVcwZUx1SCtNQW9HQ0
      NxR1NNNDlCQU1DTURVeEV6QVJCZ05WQkFvTUNrMTVRblZ6YVc1bGMzT
      XhEVEFMQmdOVkJBY01CRk5wZEdVeER6QU5CZ05WQkFNTUJsUmxjM1JE
      UVRBZUZ3MHhPVEE1TVRFd01qTTNNekphRncweU9UQTVNVEV3TWpNM01
      6SmFNRFV4RXpBUkJnTlZCQW9NQ2sxNVFuVnphVzVsYzNNeERUQUxCZ0
      5WQkFjTUJGTnBkR1V4RHpBTkJnTlZCQU1NQmxSbGMzUkRRVEJaTUJNR
      0J5cUdTTTQ5QWdFR0NDcUdTTTQ5QXdFSEEwSUFCT2t2a1RIdThRbFQz
      RkhKMVVhSTcrV3NIT2IwVVMzU0FMdEc1d3VLUURqaWV4MDYvU2NZNVB
      KaWJ2Z0hUQitGL1FUamdlbEhHeTFZS3B3Y05NY3NTeWFqUlRCRE1CSU
      dBMVVkRXdFQi93UUlNQVlCQWY4Q0FRRXdEZ1lEVlIwUEFRSC9CQVFEQ
      WdJRU1CMEdBMVVkRGdRV0JCVG9aSU16UWRzRC9qLytnWC83Y0JKdWNI
      L1htakFLQmdncWhrak9QUVFEQWdOSkFEQkdBaUVBdHhRMytJTEdCUEl
      0U2g0YjlXWGhYTnVocVNQNkgrYi9MQy9mVllEalE2b0NJUURHMnVSQ0
      hsVnEzeWhCNThUWE1VYnpIOCtPbGhXVXZPbFJEM1ZFcURkY1F3PT0if
      X0",
    "signatures": [
        {
            "protected":
              "eyJ4NWMiOlsiTUlJQmt6Q0NBVGlnQXdJQkFnSUdBV0ZCakNrWU1B
              b0dDQ3FHU000OUJBTUNNRDB4Q3pBSkJnTlZCQVlUQWtGUk1SVXdFd
              1lEVlFRS0RBeEthVzVuU21sdVowTnZjbkF4RnpBVkJnTlZCQU1NRG
              twcGJtZEthVzVuVkdWemRFTkJNQjRYRFRFNE1ERXlPVEV3TlRJME1
              Gb1hEVEk0TURFeU9URXdOVEkwTUZvd1R6RUxNQWtHQTFVRUJoTUNR
              VkV4RlRBVEJnTlZCQW9NREVwcGJtZEthVzVuUTI5eWNERXBNQ2NHQ
              TFVRUF3d2dTbWx1WjBwcGJtZERiM0p3SUZadmRXTm9aWElnVTJsbm
              JtbHVaeUJMWlhrd1dUQVRCZ2NxaGtqT1BRSUJCZ2dxaGtqT1BRTUJ
              Cd05DQUFTQzZiZUxBbWVxMVZ3NmlRclJzOFIwWlcrNGIxR1d5ZG1X
              czJHQU1GV3diaXRmMm5JWEgzT3FIS1Z1OHMyUnZpQkdOaXZPS0dCS
              Eh0QmRpRkVaWnZiN294SXdFREFPQmdOVkhROEJBZjhFQkFNQ0I0QX
              dDZ1lJS29aSXpqMEVBd0lEU1FBd1JnSWhBSTRQWWJ4dHNzSFAyVkh
              4XC90elVvUVwvU3N5ZEwzMERRSU5FdGNOOW1DVFhQQWlFQXZJYjNv
              K0ZPM0JUbmNMRnNhSlpSQWtkN3pPdXNuXC9cL1pLT2FFS2JzVkRpV
              T0iXSwidHlwIjoidm91Y2hlci1qd3MranNvbiIsImFsZyI6IkVTMj
              U2In0",
            "signature":
              "y1HLYBFlwouf42XWSKUWjeYQHnG2Q6A4bjA7hvTkB3z1dPwTUljP
              HtuN2Qex6gDxTfaSiKeoXGsOD4JWOgQJPg"
      }
   ]
}
```


Figure 4: Example Voucher Response

Authors' Addresses

Thomas Werner
Siemens AG

Email: thomas-werner@siemens.com

Michael Richardson
Sandelman Software Works

Email: mcr+ietf@sandelman.ca