

anima Working Group
Internet-Draft
Updates: [RFC8366](#) (if approved)
Intended status: Standards Track
Expires: 8 September 2022

M. Richardson
Sandelman Software Works
T. Werner
Siemens AG
7 March 2022

JWS signed Voucher Artifacts for Bootstrapping Protocols
draft-ietf-anima-jws-voucher-03

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 8 September 2022.

Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights

Internet-Draft

JWS-voucher

March 2022

and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the [Trust Legal Provisions](#) and are provided without warranty as described in the Revised BSD License.

Table of Contents

1.	Introduction	2
2.	Terminology	3
3.	JSON Web Signatures - General JWS JSON Serialization	
	Syntax	3
3.1.	Unprotected Header	4
3.2.	Protected Header	4
3.3.	Voucher Representation in General JWS JSON Serialization	
	Syntax	4
4.	Privacy Considerations	5
5.	Security Considerations	5
6.	IANA Considerations	6
6.1.	Media-Type Registry	6
6.1.1.	application/voucher-jws+json	6
7.	Changelog	6
8.	References	7
8.1.	Normative References	7
8.2.	Informative References	7
Appendix A.	Examples	9
A.1.	Example Pledge Voucher Request - PVR (from Pledge to Registrar)	9
A.2.	Example Parboiled Registrar Voucher Request - RVR (from Registrar to MASA)	10
A.3.	Example Voucher Response (from MASA to Pledge, via Registrar)	12
	Authors' Addresses	14

[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 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](#)].

Internet-Draft

JWS-voucher

March 2022

This document provides an equivalent mapping of JSON format with the signature format as JSON Web Signature (JWS) [[RFC7515](#)]. The encoding specified in this document is required for [[I-D.ietf-anima-brski-prm](#)] and may be required and/or preferred in other use cases, for example when JWS 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-prm](#)] 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 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 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 - General JWS JSON Serialization Syntax

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

[RFC7515] defines two serializations: the "JWS Compact Serialization" and the "JWS JSON Serialization".

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](#).

A JWS JSON Serialization Overview is given by [RFC7515] in [section 3.2](#) and [section 7.2.1](#) provides more details. It works out to:

```
[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": "2022-03-02T03:01:24.618Z",
      "pinned-domain-cert": "base64encodedvalue=="
    }
  },
  "signatures": [
    {
      "protected": {
        "x5c": [
          "base64encodedvalue=="
        ],
        "alg": "ES256"
      },
      "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"

[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>>.

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-02](https://www.ietf.org/archive/id/draft-ietf-anima-brski-prm-02), 4 March 2022, <<https://www.ietf.org/archive/id/draft-ietf-anima-brski-prm-02.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-16](https://www.ietf.org/archive/id/draft-ietf-anima-constrained-voucher-16), 14 February 2022, <<https://www.ietf.org/archive/id/draft-ietf-anima-constrained-voucher-16.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](https://www.ietf.org/archive/id/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](https://www.ietf.org/archive/id/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/m1r9uo4xYzn0cf85EyK0Rhut598/>>.

[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](https://www.rfc-editor.org/info/rfc5280), DOI 10.17487/RFC5280, May 2008, <<https://www.rfc-editor.org/info/rfc5280>>.

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

[RFC8792] Watsen, K., Auerswald, E., Farrell, A., and Q. Wu, "Handling Long Lines in Content of Internet-Drafts and RFCs", [RFC 8792](https://www.rfc-editor.org/info/rfc8792), 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":
    "eyJpZXRMZXZdWNoZXItcmVxdWVzdDp2b3VjaGVyIjpw7ImNyZWFOZWQtb24iOiIyMDE5LTAyLTE4VDA3OjM5OjAzLjAwMFoiLCJub25jZSI6IjU3NDI2OTg0MjI0DA0NzIifX0",
  "signatures": [
    {
      "protected":
        "eyJhbGciOiJFUzI1NiIsIng1YyI6WyJNSUwCMmpDQ0FZQ2dBd0lCQWdJR0FXZWdkY1NMTUFvR0NDcUdTTTQ5QkFNQ00EMHhDekFKQmd0VkJBWVRBa0ZSTVJVd0V3WURWUVFLREF4S2FXNW5TbWx1WjB0dmNuQXhGekFWQmd0VkJBTU1Ea3BwYm1kS2FXNW5WR1Z6ZEVOQk1DQVhEVEU0TVRJeE1qQXpNamcxTVZvWUR6azVPVGt4TWpNeE1qTTFPVFU1V2pCU01Rc3dDUVlEVlFRR0V3SkJVVGVWTVJNR0ExVUVDZ3dNU21sdVowcHBibWREYjNkd01STXdFUVlEVlFRRkV3b3dNVEl6TkRVMk56ZzVNUmN3RlFZRFZRUUREQTVLYVc1b1NtbHVhVWFJZG1sa1pUQ1pNQk1HQnlxR1NNNDlBZ0VHQ0Nxr1NNNDlBd0VIQTBJQUJNVkdHOFo1cGpmNWpYbnlyVXJYeVoxa1BncUJlM05YdTFkVEFEZStyL3Y2SnwJSWZzNTVJZ2NIQzNheHBpYnFKTS9iV1JhRXlqcWNDSmo0akprb3dDdWpWVEJUTUN3R0NTc0dBUVFCZ3U1U0FnUWZEQjF0WVh0aExYUmxjM1F1YzZJsbGJXVnVjeTFpZEM1dVpYUTZPVFEwTXpBVEJnTlZIU1VFRERBS0JnZ3JCZ0VGQ1FjREFqQU9CZ05WSFE4QkFmOEVCCU1DQjRBd0NnWUllb1pJemowRUF3SURTQUF3U1FJZ1d0UHpJSVhZMml4UlhKdEV4S0VoaFpkYTRYK0VwbFpvbUVJMNpBMGRzam9DSVFDM0pwUW1SWE1Hbi9wNEJlOWl6aWk5MmVjbFR4NC9PNHJsbTdNeUxxa2hkQT09Il19",
      "signature":
        "xURZmcWSFaBD2cNkr37azT9osWfzTZ_veCsVho3fwdD6NR4ghL61VJmY_ra0a42SvoW2Tu4XllldzzD8VDtCCDg"
    }
  ]
}
```

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":
    "eyJpZXRmLXZvdWNoZXItcmVxdWVzdDp2b3VjaGVyIjp7InNlcmhbc1
    udW1iZXIiOiIwMTIzNDU2Nzg5Iiwibm9uY2UiOiI1NzQyNjk4NDIyNjg
    wNDcyIiwicHJpb3Itc2lnbmVkbWVzdWNoZXItcmVxdWVzdCI6ImV5Snd
    ZWGXzYjJGa0lqb2laWGXLY0ZwVWVtMU1XRnAyWkZkT2IxcFlTFWJqYlZ
    aNFPgZFdIbVJFY0RkaU0xWnFZVWRXZVVscWNEZEpiVTU1V2xkR01GcFh
    VWFJpTWpScFQybEplVTFFUlRWTvZFRjVURlJGtKZaRVFUTlBhazAxVDJ
    wQmVreHFRWGR0Um05cFRFTktkV0l5TldwYVUwazJTV3BWTtA1RVNUSlB
    WR2N3VFdwSk1rOUVRVEJPZWtscFpsZ3dJaXdpYzJsbmJtRjBkWepsY3l
    JNlczc2ljSEp2ZEdWamRHVmtJam9pWlhsS2FHSkhZMmxQYVVwR1ZYcEp
    NVTvU1h0SmJtY3hXWGxKTmxkNVNrNVRWV3hEVFcxd1JGRXdSbHBSTW1
    SQ1pEQnNRMUZYWkVwU01FWllXbGRrYTFreFRrMVVWVWoyVWpCT1JHTlZ
    aRlJVVkZFMVXdEdUbEV3TVVWTLNHAEVAV3RHUzFGdFpFOvdhMHBdVjF
    aU1FtRXdXbE5VVmtwV1pEQldNMWRWVWxkVlZrWk1Va1ZHTkZNeVJsaE9
    WelZVWwXkNE1WZHFRazlrYlU1MVVWaG9SMlZyUmxkUmJXUlBwbXRlUWx
    SVk1VVmhNMEozV1cweGExTXlSbGhPvnpWwFVqRmF0bHBGVms5UmF6RkV
    VVlpvUlZaRlZUQlVWbEpLWlVVeGNWRlljRTVoYldONFZGwMfkbGRWVWp
    aaGVsWlFWa2QwTkZSWGNFNWxSVEZ4VkZSR1VGWkdWVEZXTW5CRFZUQXh
    VbU16WkVSVlZteEZWbXhHVWxJd1ZqTlRhMHBXVmtWV1YxUlZTazVTTUV
    WNFZsVldSRm96WkU1Vk1qRnpaRlp2ZDJOSVftbGlWMUpGV1dwT1MyUXd
    NVk5VV0dSR1ZWwNNSVlpzUmxKU2ExWXpZak5rVGxaRmJEWlVhMUpXVFD
    zMU5scDZWazVWYlU0elVteEdXbEpHV2xKVlZWskZVVLJXVEZsV1l6Rml
    iRTUwWWtoV1lVMUdTbk5hUnpGellXeHdWVkJzY0U1UmF6RklVVzVzZUZ
    JeFRrNU9SR3hDV2pCV1NGRXdUbmhTTVU1T1RrUnNRbVF3VmtsUlZFSkt
    VVlZLVGxacIpFaFBSbTh4WTBkd2JVNVhjRmxpYm14NVZsaEtXV1ZXYjN
    oaE1VSsnVZMVZLYkUwd05WbGtWRVpyVmtWR1JWcFRkSGxNTTFreVUyNXd
    TbE5IZDNwT1ZGWktXakpPU1ZGNlRtaGxTRUp3V1c1R1MxUlRPV2xXTVV
    wb1VsaHNjV05YVGtSVGJXOHdZV3R3Y21JelPfumtWM0JYVmtWS1ZWUlZ
    Uak5TTUu1VVL6QmtRbFZXUmtOYU0xVXhWVEJHYmxWWFdrVlJha1l3VjF
    ab1QyRkZlRmxWYlhocVRURkdNVmw2U250aVIwcFlWbTVXYW1WVVJuQmF
    SVTB4WkZad1dWVlVXbEJXUmtWM1ZGaHdRbFpGU201VWJGcEpWVEZXUmx
```



```

        iXC9MQ1wvZlZZRGpRNm9DSVFERzJ1UkNIbFZxM3loQjU4VFhNVWJ6SDg
        rT2xoV1V2T2xSRDNWRXFEZGNRdz09IloSImFsZyI6IkVTMjU2In0",
        "signature":
        "zvtnaEDpOqL49XnYVRbLxVAaZCMRtDiaLqMeFSH3UsjHdz4FT0lFywV
        7-5inMpafXTnqqxnD2Gpr3ClUXUyAJg"
    }
]
}

```

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":
    "eyJpZXRmLXZvdWNoZXI6dm91Y2hlcilI6eyJhc3NlcnRpb24iOiJsb2
    dnZWQilLCJzZXJpYWwtbnVtYmVyIjoimDEyMzQ1Njc4OStIm5vbmNlI
    joINTc0MjY5ODQyMjY4MDQ3MiIsImNyZWZ0ZWQtb24iOiIyMDIyLTAz
    LTAyVDAzOjAxOjI0LjYxOFoiLCJwaW5uZWQtZG9tYWluLWNlcnQiOiJ
    NSUlCcERDQ0FVbWdBd0lCQWdJR0FXMGVMdUgrTUFvR0NDcUdTTTQ5Qk
    FNQ01EVXhFekFSQmdOVkJBb01DazE1UW5WemFXNWxjM014RFRBTEJnT
    lZCQWNNQkZ0cGRHVXhEekFOQmdOVkJBb01DazE1UW5WemFXNWxjM014
    RFRBTEJnTlRBNU1URXdNak0zTXpKYUZ3MHlPVEE1TVRFd01qTTNnekph
    TURVeEV6QVJCZ05WQkFvTUNrMTVRbLZ6YVc1bGMzTXhEVEFMQmdOVk
    JBY01CRk5wZEdVeER6QU5CZ05WQkFNTUJsUmxjM1JEUVRCWk1CTUdCe
    XFHU0000UFnRUdDQ3FHU0000UF3RUhBMElBQk9rdmtUSHU4UWxUM0ZIS
    jFVYUk3K1dzSE9iMFVTM1NBTHRHNXd1S1FEamlleDA2L1NjWTVQSmli
    dmdIVEIrRi9RVGpnZWxIR3kxWUtwd2NOTWNzU3lhalJlUQkRNQkLHQTF
    VZE3RUlvd1FJTUFZQkFmOENBUUV3RGdZRFZSMFBBUUgVQkFRREFnSU
    VNQjBHQTFVZERnUVdCQlRvWklNeIFkc0Qvai8rZ1gvN2NCSnVjSC9Yb
    WpBS0JnZ3Foa2pPUFFRREFnTkpBREJHQLFQXR4UTMrSUxHQLBJdFN0
    NGI5V1h

```

```

oWE51aHFTUDZIK2IvTEMvZLZZRGpRNm9DSVFERzJ1UkNIbFZxM3loQj
U4VFhNVWJ6SDgrT2xoV1V2T2xSRDNWRXFEZGNRdz09In19",
"signatures": [
  {
    "protected":
      "eyJ4NWMiOlSiTUlJQmt6Q0NBVGlnQXdJQkFnSUdBV0ZCakNrWU1B
      b0dDQ3FHU0000UJBTUNNRDB4Q3pBSkJnTlZCQVlUQWtGUk1SVXdFd
      1lEVLFRS0RBeEthVzVuU21sdVowTnZjbkF4RnpBVkxJnTlZCQU1NRG
      twcGJtZEthVzVuVkdWemRFTkxJNQjRyRFRFNE1ERXlPVEV3TlRjME1
      Gb1hEVEk0TURFeU9URXdOVEkwTUZvd1R6RUxNQWtHQTfVRUJJoTUNR
      Vkv4RlRBVEJnTlZCQW9NREVwcGJtZEthVzVuUTI5eWNERXBNQ2NHQ
      TFVRUF3d2dTbWx1WjBwcGJtZERiM0p3SUZadmRXtm9aWElnVTJsbm
      JtbHVaeUJMWlhrd1dUQVRCZ2NxaGtqT1BRsUJCZ2dxaGtqT1BRTUJ
      Cd05DQUFTQzZiZUxBbWVxMVZ3Nm1RclJzOFIwWlcrNGIxR1d5ZG1X
      czJHQU1GV3diaXRmMm5JWEgzT3FIS1Z1OHMyUnZpQkd0aXZPS0dCS
      Eh0QmRpRkVaWnZiN294SXdfREFPQmdOVkhROEJBZjhFQkFNQ0I0QX
      dDZ1lJS29aSXpqMEVBd0lEU1FBd1JnSWhBSTRQWWJ4dHNzSFAyVkh
      4XC90e1VvUVVwU3N5ZEwzMERRSU5FdGN0OW1DVfHQWlFQXZJYjNv
      K0ZPM0JUbMNMNnNhSlpSQWtkN3pPdXNuXC9cL1pLT2FFS2JzVkRpV
      T0iXSwiYXNlIjo1RVMyNTYifQ",
    "signature":
      "vyge3GENm1BNcijXT5VH7A8CJWW7wPzH61u2VCfR8E9v8H8Yr3g9
      irYz4q5sYj2Un0VIh-hG_ogrZR0Tct_Vzw"
  }
]
}

```

Figure 4: Example Voucher Response

Authors' Addresses

Michael Richardson
 Sandelman Software Works
 Email: mcr+iETF@sandelman.ca

Thomas Werner
 Siemens AG
 Email: thomas-werner@siemens.com

