

ANIMA Working Group
Internet-Draft
Updates: 8366, 8995 (if approved)
Intended status: Standards Track
Expires: 19 June 2026

K. Watsen
Watsen Networks
M. Richardson, Ed.
Sandelman Software
E. Dijk
IoTconsultancy.nl
M. Pritikin
Cisco Systems
T. Eckert
Futurewei Technologies Inc.
Q. Ma
Huawei
16 December 2025

A Voucher Artifact for Bootstrapping Protocols
draft-ietf-anima-rfc8366bis-21

Abstract

This document defines a strategy to securely assign a Pledge to an Owner using an artifact signed, directly or indirectly, by the Pledge's manufacturer. This artifact is known as a "Voucher".

This document defines an artifact format as a YANG-defined JSON or CBOR document that has been signed using a variety of cryptographic systems.

The Voucher Artifact is normally generated by the Pledge's manufacturer (i.e., the Manufacturer Authorized Signing Authority (MASA)).

This document updates RFC8366: it includes a number of desired extensions into the YANG module. The Voucher Request YANG module defined in RFC8995 is also updated and now included in this document, as well as other YANG extensions needed for variants of BRSKI/RFC8995.

About This Document

This note is to be removed before publishing as an RFC.

Status information for this document may be found at
<https://datatracker.ietf.org/doc/draft-ietf-anima-rfc8366bis/>.

Discussion of this document takes place on the anima Working Group mailing list (<mailto:anima@ietf.org>), which is archived at <https://mailarchive.ietf.org/arch/browse/anima/>. Subscribe at <https://www.ietf.org/mailman/listinfo/anima/>.

Source for this draft and an issue tracker can be found at <https://github.com/anima-wg/voucher>.

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 19 June 2026.

Copyright Notice

Copyright (c) 2025 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 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	3
2. Terminology	5
3. Requirements Language	7
4. Survey of Voucher Types	7
5. Changes since RFC8366	9
5.1. Attempts and motivation to extend RFC8366	10
5.2. Informational Model changes since RFC8366	11

6.	Signature mechanisms	11
6.1.	CMS Format Voucher Artifact	11
7.	Voucher Artifact	12
7.1.	Tree Diagram	13
7.2.	Examples	14
7.3.	YANG Module	16
7.4.	ietf-voucher SID values	23
7.5.	Voucher Extensions	25
7.6.	Manufacturer Private Extensions	26
8.	Voucher Request Artifact	26
8.1.	Tree Diagram	26
8.2.	"ietf-voucher-request" Module	27
8.3.	ietf-voucher-request SID values	32
9.	Design Considerations	33
9.1.	Renewals Instead of Revocations	33
9.2.	Voucher Per Pledge	34
10.	Security Considerations	35
10.1.	Clock Sensitivity	35
10.2.	Protect MASA Signing Key in HSM	35
10.3.	Test Domain Certificate Validity When Signing	35
10.4.	YANG Module Security Considerations	36
11.	IANA Considerations	36
11.1.	The IETF XML Registry	36
11.2.	The YANG Module Names Registry	36
11.3.	The Media Types Registry	37
11.4.	The SMI Security for S/MIME CMS Content Type Registry	37
11.5.	The Voucher Extensions Registry	37
12.	References	38
12.1.	Normative References	38
12.2.	Informative References	40
Appendix A.	Examples	43
A.1.	Key pairs associated with examples	43
A.2.	Example CMS-signed Voucher Request	48
A.3.	Example CMS-signed Voucher from MASA	49
A.4.	Example JWS-signed Voucher from MASA	50
	Acknowledgements	51
	Authors' Addresses	52

1. Introduction

This document defines a strategy to securely assign a candidate device (Pledge) to an Owner using an artifact signed, directly or indirectly, by the Pledge's manufacturer, i.e., the Manufacturer Authorized Signing Authority (MASA). This artifact is known as the "Voucher".

The Voucher Artifact is a JSON [RFC8259] document that conforms with a data model described by YANG [RFC7950]. It may also be serialized to CBOR [CBOR]. It is encoded using the rules defined in [RFC7951] or [RFC9254], and is signed using (by default) a CMS structure [RFC5652].

The primary purpose of a Voucher is to securely convey a trust anchor that a Pledge can use to authenticate subsequent interactions. The trust anchor may be in the form of a certificate (the 'pinned-domain-cert' Attribute), a hash of a certificate, or it can be a raw public key (in constrained use cases).

This trust anchor represents the authority of the Owner of a network. Communicating this trust anchor securely to the Pledge is the job of the Voucher Artifact. The act of communicating this trust anchor is known as pinning the trust anchor, as the Pledge can then use the resulting anchor to authenticate other actors who are part of the network. The collection of all these actors is collectively known as the Domain. (This is not related to the domain name system, but rather the term is of mathematical origin)

A Voucher may be useful in several contexts, but the driving motivation herein is to support secure Onboarding mechanisms. This is accomplished by assigning an Owner to the Pledge, enabling it to authenticate the network that it is connected to.

[RFC8366] originally defined the Voucher as the only Voucher Artifact, leaving the Voucher Request that is used in BRSKI to be defined in [BRSKI]. This document includes both Voucher and Voucher Request, and therefore updates [BRSKI].

YANG is not easily extended except by updating the YANG module definition. Since [RFC8366] was written, the common pattern is to publish YANG modules as two documents: one with only the YANG module, and the other one with usage, motivation and further explanation. This allows the YANG module to be updated without replacing all of the context. This document does not follow that pattern, but future documents may update only the YANG module.

This document introduces a mechanism to support future extensions without requiring the YANG module to be revised. This includes both a new IETF standard mechanism for extensions modeled after the mechanism present in [RFC8520], as well as a facility for manufacturer private extensions.

The lifetimes of Vouchers may vary. In some Onboarding protocols, the Vouchers may include a nonce restricting them to a single use, whereas the Vouchers in other Onboarding protocols may have an

indicated lifetime. In order to support long lifetimes, this document recommends using short lifetimes with programmatic renewal, see Section 9.1.

Some Onboarding protocols using the Voucher Artifact defined in this document include: [ZERO-TOUCH], [SECUREJOIN], [BRSKI] and [cBRSKI].

2. Terminology

This document uses and defines the following terms. They are used in this document and related documents.

(Voucher) Artifact: Used throughout this document to represent a Voucher or Voucher Request as instantiated in the form of a signed datastructure. The payload of the signed datastructure is called the Voucher Data.

Attribute: A single named data element that can be stored in Voucher Data. The element's name and data type are defined by one of the YANG models as defined in this document.

Bootstrapping: The process where a Pledge obtains cryptographic key material to identify and trust future interactions within a specific Domain network. Based on imprinted key material provided during the manufacturing process (see: Imprint). This term was used in [RFC8366], but has been supplanted by the term Onboarding.

Domain: The set of entities or infrastructure under common administrative control. The goal of the Onboarding protocol is to enable a Pledge to join a Domain and obtain domain-specific security credentials. This term is not related to "DNS domain" [RFC9499] although a Domain might be associated to a specific DNS domain.

Imprint: The process where a device obtains the cryptographic key material to identify and trust future interactions generally as part of the manufacturing. This term is taken from Konrad Lorenz's work in biology with new ducklings: "during a critical period, the duckling would assume that anything that looks like a mother duck is in fact their mother" [Stajano99theresurrecting]. An equivalent for a device is to obtain the fingerprint of the manufacturer's root certification authority (root CA) certificate. A device that Imprints on an attacker suffers a similar fate to a duckling that imprints on a hungry wolf. Imprinting is a term from psychology and ethology, as described in [imprinting].

Join Registrar (and Coordinator): A representative of the Domain

that is configured, perhaps autonomically, to decide whether a new device is allowed to join the Domain. The administrator of the Domain interfaces with a Join Registrar (and Coordinator) to control this process. Typically, a Join Registrar is "inside" its Domain. For simplicity, this document often refers to this as just "Registrar".

MASA (Manufacturer Authorized Signing Authority): The entity that, for the purpose of this document, issues and signs the Vouchers for a manufacturer's Pledges and keeps logs of Pledge ownership. In some Onboarding protocols, the MASA may have an Internet presence and be integral to the Onboarding process, whereas in other protocols the MASA may be an offline service that has no active role in the Onboarding process.

Malicious Registrar: An on-path active attacker that presents itself as a legitimate Registrar.

Onboarding: Onboarding describes the process to provide necessary operational data to a Pledge and to complete the process of bringing the Pledge into an operational state. This data may include configuration data, but specifically deals with application-specific cryptographic key material (application-specific security credentials). Since [RFC8366], this term has replaced the term Bootstrapping.

Owner: The entity that controls the private key of the trust anchor conveyed by the Voucher. Typically, the Owner is indicated by the 'pinned-domain-cert' Attribute.

Pledge: The prospective component/device attempting to find and securely join a Domain. When shipped or in factory reset mode, it only trusts authorized representatives of the manufacturer.

Registrar: See Join Registrar. This term is not related to the term DNS Registrar [RFC9499].

TOFU (Trust on First Use): When a Pledge makes no security decisions but rather simply trusts the first Domain entity it is contacted by. Used similarly to [RFC7435]. This is also known as the "resurrecting duckling" model [Stajano99theresurrecting].

Voucher: A Voucher Artifact, not a Voucher Request, that is a signed statement from the MASA service that indicates to a Pledge the cryptographic identity of the Domain it should trust. When clarity is needed, it may be preceded by the type of the signature, such as CMS, JWS or COSE.

Voucher Data: The raw (serialized) representation of the YANG data elements of a Voucher (Request) without any enclosing signature. Current serialization formats include JSON and CBOR.

Voucher Request: A signed artifact sent from the Pledge to the Registrar, or from the Registrar to the MASA, for Voucher acquisition. When clarity is needed, it may be preceded by the type of the signature, such as CMS, JWS or COSE.

Pledge Voucher Request (PVR): A signed artifact sent from the Pledge to the Registrar. It is a specific form of Voucher Request.

Registrar Voucher Request (RVR): A signed artifact sent from the Registrar to the MASA. It is a specific form of Voucher Request.

3. Requirements Language

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.

4. Survey of Voucher Types

A Voucher is a cryptographically protected statement to the Pledge authorizing a zero-touch Onboarding with the Join Registrar of the Domain. The specific information a Voucher provides is influenced by the Onboarding use case.

The Voucher can convey the following information to the Join Registrar and to the Pledge:

Assertion Basis: Indicates the method that protects the Onboarding (this is distinct from the Voucher signature that protects the Voucher itself). Methods include manufacturer-asserted ownership verification, assured logging operations, or reliance on Pledge behavior such as secure or measured boot. The Join Registrar uses this information to make a determination as to whether to accept the Pledge into the network. Only some methods are normatively defined in this document. Other methods are left for future work.

Authentication of Join Registrar: Indicates how the Pledge can authenticate the Join Registrar. This document defines a mechanism to pin the Domain certificate, or a raw public key. Pinning a symmetric key, or CN-ID ([RFC6125]) or DNS-ID information (as defined in [RFC9525]) is left for future work.

Anti-Replay Protections: Time- or nonce-based information to constrain the Voucher to specific time periods or Onboarding attempts.

A number of Onboarding scenarios can be met using differing combinations of this information. All scenarios address the primary threat of an on-path active attacker (or MiTM) impersonating the Registrar. If successful, this would gain control over the Pledge. The following combinations are "types" of Vouchers:

Voucher Type	Assertion		Registrar ID		Validity	
	Logged	Verified	Trust Anchor	CN-ID or DNS-ID	RTC	Nonce
Audit Voucher	X		X			X
Nonceless Audit	X		X		X	
Owner Audit	X	X	X		X	X
Owner ID Voucher		X	X	X	X	
Bearer Voucher	X		wildcard	wildcard	optional	opt

Table 1: Overview of Voucher types

NOTE: The "RTC" column denotes Voucher validation using a Real-Time Clock.

NOTE: All Voucher types include a "Pledge ID serial-number" (column not shown for space reasons).

Audit Voucher: An audit Voucher is named after the logging assertion mechanisms that the Registrar then "audits" to enforce its local policy. The Registrar mitigates the risk of a Malicious Registrar by auditing that no unknown Registrar, or known Malicious Registrar, appears in the MASA's log entries for the Pledge. This does not directly prevent a Malicious Registrar but provides a response mechanism that ensures the on-path attack is

unsuccessful. An advantage is that actual ownership knowledge (i.e., sales integration providing an indication of who purchased the device) is not required on the MASA service.

Nonceless Audit Voucher: An audit Voucher with a validity period statement, but no guarantee of freshness. Fundamentally, it is the same as an audit Voucher except that it can be issued in advance to support network partitions or to provide a permanent Voucher for remote deployments. Being issued in advance of the Pledge being online, the Pledge can not rely on a nonce to be included for freshness. This compromise in reducing the freshness allows for the resulting Voucher to be carried across air-gapped infrastructure. In addition, if the validity period has been set sufficiently long, the Voucher can be used after the manufacturer (and its delegates) has gone out of business.

Ownership Audit Voucher: An audit Voucher where the MASA service has verified the Registrar as the authorized Owner. The MASA service mitigates a MiTM Registrar by refusing to generate audit Vouchers for unauthorized Registrars. The Registrar uses audit techniques to supplement the MASA. This provides an ideal sharing of policy decisions and enforcement between the vendor and the Owner.

Ownership ID Voucher: Named after inclusion of the Pledge's CN-ID or DNS-ID within the Voucher. The MASA service mitigates a MiTM Registrar by identifying the specific Registrar (via PKIX [RFC5280]) authorized to own the Pledge.

Bearer Voucher: A bearer Voucher is named after the inclusion of a Registrar ID wildcard. Because the Registrar identity is not indicated, this Voucher type must be treated as a secret and protected from exposure as any 'bearer' of the Voucher can claim the Pledge. This variation is included in the above table in order to clearly show how other Voucher types differ. This specification does not support bearer Vouchers at this time. There are other specifications in the industry which are equivalent though. Publishing a nonceless bearer Voucher effectively turns the specified Pledge into a TOFU device with minimal mitigation against MiTM Registrars. Bearer Vouchers are therefore out of scope.

5. Changes since RFC8366

5.1. Attempts and motivation to extend RFC8366

[RFC8366] was published in 2018 during the development of [BRSKI], [ZERO-TOUCH] and other work-in-progress efforts. Since then the industry has matured significantly, and the in-the-field activity which this document supports has become known as `_Onboarding_` rather than `_Bootstrapping_`.

The focus of [BRSKI] was Onboarding of ISP and Enterprise owned wired routing and switching equipment, with IoT devices being a less important aspect. [ZERO-TOUCH] has focused upon Onboarding of CPE equipment like cable modems and other larger IoT devices, again with smaller IoT devices being of lesser importance.

Since [BRSKI] was published there is now a mature effort to do application-level Onboarding of constrained IoT devices defined by the Thread Group and the Fairhair Alliance (now OCF) [fairhair]. The [cBRSKI] document has defined a version of [BRSKI] that is usable over constrained IEEE 802.15.4 6LoWPAN networks using CoAP and DTLS, while [I-D.ietf-lake-authz] provides for using CoAP and EDHOC on even more constrained devices with very constrained networks.

[PRM] has created a new methodology for Onboarding that does not depend upon a synchronous connection between the Pledge and the Registrar. This mechanism uses a mobile Registrar agent that works to collect and transfer signed artifacts via physical travel from one network to another.

Both [cBRSKI] and [PRM] require extensions to the Voucher Request and the resulting Voucher. The new Attributes are required to carry the additional data and describe the extended semantics. In addition [cBRSKI] uses the serialization mechanism described in [RFC9254] to produce significantly more compact artifacts.

When the process to define [cBRSKI] and [PRM] was started, there was a belief that the appropriate process was to use the [RFC7950] `_augment_` mechanism to further extend both the Voucher Request [BRSKI] and Voucher [RFC8366] artifacts. However, [PRM] needs to extend an enumerated type with additional values and `_augment_` can not do this, so that was initially the impetus for this document.

An attempt was then made to determine what would happen if one wanted to have a constrained version of the [PRM] Voucher Artifact. The result was invalid YANG, with multiple definitions of the core Attributes from the [RFC8366] Voucher Artifact. After some discussion, it was determined that the `_augment_` mechanism did not work for this use case, nor did it work better when the [RFC8040] "yang-data" extension was replaced with the [RFC8791] "structure" extension.

After significant discussion the decision was made to simply roll all of the needed extensions into this document.

5.2. Informational Model changes since RFC8366

This document therefore represents a merge of YANG definitions from [RFC8366], the Voucher Request from [BRSKI], and extensions to each of these from [cBRSKI], [CLOUD] and [PRM]. The difficulty with this approach is that the semantics of the definitions needed for the other documents is not included in this document, but rather in the respective other documents.

6. Signature mechanisms

Three signature systems have been defined for Vouchers Artifacts.

[cBRSKI] defines a mechanism that uses COSE [COSE], with the Voucher Data encoded using [RFC9254]. However, as the SID [RFC9254] allocation process requires up-to-date YANG, the SID values for this mechanism are presented in this document.

[jBRSKI] defines a mechanism that uses JSON [RFC8259] and [JWS].

The CMS signing mechanism first defined in [RFC8366] continues to be defined here.

6.1. CMS Format Voucher Artifact

The IETF evolution of PKCS#7 is CMS [RFC5652]. A CMS-signed Voucher, the default type, contains a ContentInfo structure with the Voucher Data. An OID for JSON-encoded Voucher Data is allocated in Section 11.4, and it is to be placed in the 'eContentType' field in the ContentInfo.

The signing structure is a CMS SignedData structure, as specified by Section 5.1 of [RFC5652], encoded using ASN.1 Distinguished Encoding Rules (DER), as specified in ITU-T X.690 [ITU-T.X690.2015].

[RFC5652] mandates that SignedAttributes MUST be present when the content type is not 'id-data'. This mitigates attacks on CMS as described in [I-D.vangeest-lamps-cms-euf-cma-signeddata]. Decoders MUST verify that SignedAttributes are present.

To facilitate interoperability, Section 11.3 the media type "application/voucher-cms+json" and the filename extension ".vcj" were registered by [RFC8366].

The CMS structure MUST contain a 'signerInfo' structure, as described in Section 5.1 of [RFC5652], containing the signature generated over the content using a private key trusted by the recipient. Normally, the recipient is the Pledge and the signer is the MASA. In the Voucher Request, the signer is the Pledge (in the PVR), or the Registrar (in the RVR).

Note that Section 5.1 of [RFC5652] includes a discussion about how to validate a CMS object, which is really a PKCS7 object (cmsVersion=1). Intermediate systems (such as the Bootstrapping Remote Secure Key Infrastructures [BRSKI] Registrar) that might need to evaluate the Voucher in flight MUST be prepared for such an older format. No signaling of the format version is necessary, as the manufacturer knows the capabilities of the Pledge and will use an appropriate format Voucher for each Pledge.

The CMS structure SHOULD also contain all of the certificates leading up to and including the signer's trust anchor certificate known to the recipient. The inclusion of the trust anchor is unusual in many applications, but third parties cannot accurately audit the transaction without it.

The CMS structure MAY also contain revocation objects for any intermediate certificate authorities (CAs) between the Voucher issuer and the trust anchor known to the recipient. However, the use of CRLs and other validity mechanisms is discouraged, as the Pledge is unlikely to be able to perform online checks and is unlikely to have a trusted clock source. As described below, the use of short-lived Vouchers and/or a Pledge-provided nonce provides a freshness guarantee.

7. Voucher Artifact

The Voucher's primary purpose is to securely assign a Pledge to an Owner. The Voucher informs the Pledge which entity it should consider to be its Owner.

This document defines a Voucher Artifact that is a CMS-signed encoding of the JSON-encoded Voucher Data as defined by the YANG module Section 7.3. Also, this document defines Voucher Data that is CBOR-encoded based on the same YANG model. The CBOR-encoded (signed) Voucher based on this CBOR Voucher Data is defined in [cBRSKI].

The Voucher Data format is described here as a practical basis for some uses (such as in NETCONF), but more to clearly indicate what Vouchers look like in practice. This description also serves to validate the YANG data model.

[RFC8366] defined a media type and a filename extension for the CMS-encoded JSON type. The media type for JOSE format Vouchers is defined in [jBRSKI] and the media type for COSE format Vouchers is defined in [cBRSKI]. Both include respective filename extensions.

The media type is used by the Pledge (requesting to the Registrar) and by the Registrar (requesting to the MASA) to signal what Voucher format is expected. Other aspects of the Voucher, such as it being nonceless or which kind of pinned anchor is used, are not part of the media type.

Only the format of Voucher that is expected is signaled in the form of a (MIME) media type in the HTTP "Accept" header [RFC9110].

For Vouchers stored/transferred via methods like a USB storage device (USB key), the Voucher format is usually signaled by a filename extension.

7.1. Tree Diagram

The following tree diagram illustrates a high-level view of a Voucher document. The notation used in this diagram is described in [RFC8340]. Each node in the diagram is fully described by the YANG module in Section 7.3. Please review the YANG module for a detailed description of the Voucher format.

```
module: ietf-voucher

structure voucher:
  +-- created-on?                yang:date-and-time
  +-- extensions*                union
  +-- manufacturer-private?      binary
  +-- assertion?                 enumeration
  +-- serial-number              string
  +-- idevid-issuer?             binary
  +-- pinned-domain-cert?        binary
  +-- pinned-domain-pubk?        binary
  +-- pinned-domain-pubk-sha256? binary
  +-- domain-cert-revocation-checks? boolean
  +-- last-renewal-date?         yang:date-and-time
  +-- expires-on?                yang:date-and-time
  +-- nonce?                     binary
  +-- est-domain?                ietf:uri
  +-- additional-configuration-url? ietf:uri
```

7.2. Examples

This section provides Voucher Data examples for illustration purposes. These examples conform to the JSON encoding rules defined in [RFC8259].

The following example illustrates an ephemeral Voucher (uses a nonce). The MASA generated this Voucher using the 'logged' assertion type, knowing that it would be suitable for the Pledge making the request.

```
{
  "ietf-voucher:voucher": {
    "created-on": "2016-10-07T19:31:42Z",
    "assertion": "logged",
    "serial-number": "JADA123456789",
    "idevid-issuer": "base64encodedvalue==",
    "pinned-domain-cert": "base64encodedvalue==",
    "nonce": "base64encodedvalue=="
  }
}
```

The following example illustrates a non-ephemeral Voucher (containing no nonce, or "nonceless"). While the Voucher itself expires after two weeks, it presumably can be renewed for up to a year. The MASA generated this Voucher using the 'verified' assertion type, which should satisfy all Pledges.

```
{
  "ietf-voucher:voucher": {
    "created-on": "2016-10-07T19:31:42Z",
    "expires-on": "2016-10-21T19:31:42Z",
    "assertion": "verified",
    "serial-number": "JADA123456789",
    "idevid-issuer": "base64encodedvalue==",
    "pinned-domain-cert": "base64encodedvalue==",
    "domain-cert-revocation-checks": true,
    "last-renewal-date": "2017-10-07T19:31:42Z"
  }
}
```

The final two examples illustrate a Voucher that includes an (example) extension per Section 7.5. The hypothetical YANG module name of the extension is "example-my-extension". First, a JSON serialization is shown.

```
{
  "ietf-voucher:voucher": {
    "created-on": "2016-10-07T19:31:42Z",
    "assertion": "logged",
    "serial-number": "JADA123456789",
    "idevid-issuer": "base64encodedvalue==",
    "pinned-domain-cert": "base64encodedvalue==",
    "nonce": "base64encodedvalue==",
    "extensions": ["example-my-extension"],
    "extension:example-my-extension": {
      "my-ext-leaf1": "my-ext-leaf1-data"
    }
  }
}
```

Next, a CBOR serialization is shown in CBOR diagnostic notation. This uses again the extension module 'example-my-extension' and refers to it using its SID value 305823299950. Note that for this example, long binary strings are abbreviated using the ellipsis (...) notation.

```

{
  2451: {
    2: "2016-10-07T19:31:42Z", / ietf-voucher:voucher /
    1: 1, / created-on /
    11: "JADA123456789", / assertion (logged) /
    5: h'04183016 ... 1736C3E0', / serial-number /
    8: h'30820122 ... 12328CFF', / idevid-issuer /
    7: h'831D5198A6CA2C7F', / pinned-domain-cert /
    17: [305823299950], / nonce /
    47(305823299950): { / extensions /
      1: "my-ext-leaf1-data" / example-my-extension /
    } / my-ext-leaf1 /
  }
}

```

[jBRSKI], Section 8 contains examples of Vouchers encoded in JSON, and signed with [JWS]. [cBRSKI], Section 9 contains examples of Vouchers encoded in CBOR, and signed with [COSE].

7.3. YANG Module

During development of this merged YANG module, advice was given to better organize mutually exclusive Attributes such as 'pinned-domain-cert' vs 'pinned-domain-pubk', or 'expires-on' vs 'nonce'. Unfortunately, [CORESID] does not explain how and why choice statements are assigned SID values, and the tooling as of the end of 2025 is inconsistent with both the document, and the intuitive notions as to how this should work. As the simplest way forward, the choice mechanisms that were introduced have been commented out in the YANG, allowing the SID values to be generated correctly. As a result, the SID values presented in Section 7.4 and Section 8.3 are to be considered normative, rather than relying exclusively on the ".sid" file [CORESID] generated from the YANG modules. The presented SID values are believed to be correct, but future reprocessing of the YANG module to a ".sid" file could result in changes as the tooling is fixed. Any such changes will be recorded as errata on this document.

```

<CODE BEGINS> file "ietf-voucher@2021-07-02.yang"
module ietf-voucher {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:ietf-voucher";
  prefix vch;

  import ietf-yang-types {
    prefix yang;
    reference
      "RFC 6991: Common YANG Data Types";
  }

```



```
}
import ietf-inet-types {
  prefix ietf;
  reference
    "RFC 6991: Common YANG Data Types";
}
import ietf-yang-structure-ext {
  prefix sx;
}

organization
  "IETF ANIMA Working Group";
contact
  "WG Web:    <https://datatracker.ietf.org/wg/anima/>
  WG List:    <mailto:anima@ietf.org>
  Author:     Kent Watsen
               <mailto:kent+ietf@watsen.net>
  Author:     Michael Richardson
               <mailto:mcr+ietf@sandelman.ca>
  Author:     Max Pritikin
               <mailto:pritikin@cisco.com>
  Author:     Toerless Eckert
               <mailto:tte@cs.fau.de>
  Author:     Qiufang Ma
               <mailto:maqiufang1@huawei.com>
  Author:     Esko Dijk
               <mailto:esko.dijk@iotconsultancy.nl>";

description
  "This module defines the format for a Voucher, which is
  produced by a pledge's manufacturer or delegate (MASA)
  to securely assign a pledge to an 'owner', so that the
  pledge may establish a secure connection to the owner's
  network infrastructure.

  Copyright (c) 2023 IETF Trust and the persons identified as
  authors of the code.  All rights reserved.

  Redistribution and use in source and binary forms, with or
  without modification, is permitted pursuant to, and subject to
  the license terms contained in, the Revised BSD License set
  forth in Section 4.c of the IETF Trust's Legal Provisions
  Relating to IETF Documents
  (https://trustee.ietf.org/license-info).

  This version of this YANG module is part of RFC XXXX
  (https://www.rfc-editor.org/info/rfcXXXX); see the RFC itself
  for full legal notices.
```

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 (RFC 2119) (RFC 8174) when, and only when, they appear in all capitals, as shown here.";

```
// RFCEDITOR: please replace XXXX in this entire code fragment
// with the RFC number assigned and remove this notice.
```

```
revision 2023-01-10 {
  description
    "Updates and additions described by RFC XXXX";
  reference
    "RFC XXXX A Voucher Profile for Bootstrapping Protocols";
}
revision 2018-05-09 {
  description
    "Initial version";
  reference
    "RFC 8366: Voucher Profile for Bootstrapping Protocols";
}

grouping voucher-artifact-grouping {
  description
    "Grouping to allow reuse/extensions in future work.";
  leaf created-on {
    type yang:date-and-time;
    description
      "A value indicating the date this voucher was created.
      This node is primarily for human consumption and auditing.
      Future work MAY create verification requirements based on
      this node.";
  }
  leaf-list extensions {
    type union {
      type uint64; // when serialized to CBOR with SID
      type string; // when serialized to CBOR or JSON
    }
    description
      "A list of extension names that are used in this Voucher
      file. Each name is registered with the IANA. Standard
      extensions are described in an RFC, while vendor proprietary
      ones are not.";
  }
  leaf manufacturer-private {
    type binary;
    description
      "In CBOR serialization, this is a CBOR bstr containing any
```

```
    valid CBOR that the manufacturer wishes to share with its
    pledge. In JSON serializations, this contains additional
    JSON instead, and it is base64URL encoded.";
  }
  leaf assertion {
    type enumeration {
      enum verified {
        value 0;
        description
          "Indicates that the ownership has been positively
          verified by the MASA (e.g., through sales channel
          integration).";
      }
      enum logged {
        value 1;
        description
          "Indicates that the voucher has been issued after
          minimal verification of ownership or control. The
          issuance has been logged for detection of
          potential security issues (e.g., recipients of
          vouchers might verify for themselves that unexpected
          vouchers are not in the log). This is similar to
          unsecured trust-on-first-use principles but with the
          logging providing a basis for detecting unexpected
          events.";
      }
      enum proximity {
        value 2;
        description
          "Indicates that the voucher has been issued after
          the MASA verified a proximity proof provided by the
          device and target domain. The issuance has been
          logged for detection of potential security issues.";
      }
      enum agent-proximity {
        value 3;
        description
          "Mostly identical to proximity, but
          indicates that the voucher has been issued
          after the MASA has verified a statement that
          a registrar agent has made contact with the device.";
      }
    }
    description
      "The assertion is a statement from the MASA regarding how
      the owner was verified. This statement enables pledges
      to support more detailed policy checks. Pledges MUST
      ensure that the assertion provided is acceptable, per
```

```
        local policy, before processing the voucher.";
    }
    leaf serial-number {
        type string;
        mandatory true;
        description
            "The serial-number of the hardware.  When processing a
            voucher, a pledge MUST ensure that its serial-number
            matches this value.  If no match occurs, then the
            pledge MUST NOT process this voucher.";
    }
    leaf idevid-issuer {
        type binary;
        description
            "The Authority Key Identifier OCTET STRING (as defined in
            Section 4.2.1.1 of RFC 5280) from the pledge's IDevID
            certificate.  Optional since some serial-numbers are
            already unique within the scope of a MASA.
            Inclusion of the statistically unique key identifier
            ensures statistically unique identification of the
            hardware.
            When processing a voucher, a pledge MUST ensure that its
            IDevID Authority Key Identifier matches this value.  If no
            match occurs, then the pledge MUST NOT process this
            voucher.
            When issuing a voucher, the MASA MUST ensure that this
            field is populated for serial-numbers that are not
            otherwise unique within the scope of the MASA.";
    }
    // choice pinning {
    //   description "One of these attributes is used by the
    //               MASA to pin the registrar identity";
    leaf pinned-domain-cert {
        type binary;
        description
            "An X.509 v3 certificate structure, as specified by
            RFC 5280, using Distinguished Encoding Rules (DER)
            encoding, as defined in ITU-T X.690.

            This certificate is used by a pledge to trust a Public Key
            Infrastructure in order to verify a domain certificate
            supplied to the pledge separately by the bootstrapping
            protocol.  The domain certificate MUST have this
            certificate somewhere in its chain of certificates.
            This certificate MAY be an end-entity certificate,
            including a self-signed entity.";
        reference
            "RFC 5280:"
```

```
Internet X.509 Public Key Infrastructure Certificate
and Certificate Revocation List (CRL) Profile.
ITU-T X.690:
Information technology - ASN.1 encoding rules:
Specification of Basic Encoding Rules (BER),
Canonical Encoding Rules (CER) and Distinguished
Encoding Rules (DER).";
}
leaf pinned-domain-pubk {
  type binary;
  description
    "The pinned-domain-pubk may replace the
    pinned-domain-cert in constrained uses of
    the voucher. The pinned-domain-pubk
    is the Raw Public Key of the registrar.
    This field is encoded as a Subject Public Key Info block
    as specified in RFC7250, in section 3.
    The ECDSA algorithm MUST be supported.
    The EdDSA algorithm as specified in
    draft-ietf-tls-rfc4492bis-17 SHOULD be supported.
    Support for the DSA algorithm is not recommended.
    Support for the RSA algorithm is a MAY.";
}
leaf pinned-domain-pubk-sha256 {
  type binary;
  description
    "The pinned-domain-pubk-sha256 is a second
    alternative to pinned-domain-cert. In many cases the
    public key of the domain has already been transmitted
    during the key agreement process, and it is wasteful
    to transmit the public key another two times.
    The use of a hash of public key info, at 32-bytes for
    sha256 is a significant savings compared to an RSA
    public key, but is only a minor savings compared to
    a 256-bit ECDSA public-key.
    Algorithm agility is provided by extensions to this
    specification which can define a new leaf for another
    hash type.";
}
// } choice pinning removed
leaf domain-cert-revocation-checks {
  type boolean;
  description
    "A processing instruction to the pledge that it MUST (true)
    or MUST NOT (false) verify the revocation status for the
    pinned domain certificate. If this field is not set, then
    normal PKIX behavior applies to validation of the domain
    certificate.";
```

```
}
leaf last-renewal-date {
  type yang:date-and-time;
  must '../expires-on';
  description
    "The date that the MASA projects to be the last date
    it will renew a voucher on. This field is merely
    informative; it is not processed by pledges.

    Circumstances may occur after a voucher is generated that
    may alter a voucher's validity period. For instance,
    a vendor may associate validity periods with support
    contracts, which may be terminated or extended
    over time.";
}
//choice nonceless {
//  description "Either a nonce must be present,
//              or an expires-on header";
leaf expires-on {
  type yang:date-and-time;
  description
    "A value indicating when this voucher expires. The node is
    optional as not all pledges support expirations, such as
    pledges lacking a reliable clock.

    If this field exists, then the pledges MUST ensure that
    the expires-on time has not yet passed. A pledge without
    an accurate clock cannot meet this requirement.

    The expires-on value MUST NOT exceed the expiration date
    of any of the listed 'pinned-domain-cert' certificates.";
}
leaf nonce {
  type binary {
    length "8..32";
  }
  description
    "A value that can be used by a pledge in some bootstrapping
    protocols to enable anti-replay protection. This node is
    optional because it is not used by all bootstrapping
    protocols.

    When present, the pledge MUST compare the provided nonce
    value with another value that the pledge randomly
    generated and sent to a bootstrap server in an earlier
    bootstrapping message. If the value is present, but
    the values do not match, then the pledge MUST NOT process
    this voucher.";
```

```
}
// } choice nonceless
leaf est-domain {
  type ietf:uri;
  description
    "The est-domain is a URL from which the pledge should
    continue doing enrollment rather than with the
    cloud registrar.
    The pinned-domain-cert contains a trust-anchor
    which is to be used to authenticate the server
    found at this URI.";
}
leaf additional-configuration-url {
  type ietf:uri;
  description
    "The additional-configuration attribute contains a
    URL to which the pledge can retrieve additional
    configuration information.
    The contents of this URL are manufacturer specific.
    This is intended to do things like configure
    a VoIP phone to point to the correct hosted
    PBX, for example.";
}
}

// Top-level statement
sx:structure voucher {
  uses voucher-artifact-grouping;
}
}
<CODE ENDS>
```

7.4. ietf-voucher SID values

[RFC9254] explains how to serialize YANG into CBOR, and for this a series of SID values are required. The below SID values are assigned to the 'ietf-voucher' YANG module elements and are considered normative.

The right column shows the XPath expression for the YANG data node to which the SID value is assigned. In the XPath, the ellipsis (...) notation is used to abbreviate the structure path '/ietf-voucher:voucher' to let each entry fit on one line.

SID Assigned to

```

-----
2450 module ietf-voucher
2451 data    /ietf-voucher:voucher
2452 data    .../assertion
2453 data    .../created-on
2454 data    .../domain-cert-revocation-checks
2455 data    .../expires-on
2456 data    .../idevid-issuer
2457 data    .../last-renewal-date
2458 data    .../nonce
2459 data    .../pinned-domain-cert
2460 data    .../pinned-domain-pubk
2461 data    .../pinned-domain-pubk-sha256
2462 data    .../serial-number
2463 data    .../additional-configuration-url
2464 data    .../est-domain
2465 data    .../manufacturer-private
2466 data    .../extensions

```

The 'assertion' Attribute is an enumerated type in [RFC8366], but no values were provided as part of the enumeration. This document provides enumerated values as part of the YANG module.

In the JSON serialization, the literal strings from the enumerated types are used so there is no ambiguity.

In the CBOR serialization, a small integer is used, and the enumeration values are repeated here for convenience. However, the YANG module should be considered authoritative. No IANA registry is provided or necessary because the YANG module (and this document) would be extended when there are new entries required.

CBOR Integer	Assertion Type
0	verified
1	logged
2	proximity
3	agent-proximity

Table 2: CBOR integers for the
'assertion' Attribute enum
value

7.5. Voucher Extensions

An unstated assumption in [RFC8366] was that Vouchers could be extended in proprietary ways by manufacturers. This allows for manufacturers to communicate new things from the MASA to the Pledge, and since both are under control of the same entity, it seemed perfectly fine, even though it would violate the strict definition of the YANG model.

The JSON serialization of Vouchers implicitly accomodates the above, since the Voucher is just a map (or dictionary). Map keys are just strings, and creating unique strings is easy to do by including the manufacturer's DNS domain name.

In CBOR serialization [RFC9254], the situation is not so easy when SID keys are used. An extension might need to use "Private range" [CORESID] SID values, or acquire SID values for their own use.

Where the process has become complex is when making standard extensions, as has happened recently, resulting in this document. The processes which were anticipated to be useful (the YANG "augment" mechanism), turned out not to be, see Section 5.1.

Instead, a process similar to what was done by [RFC8520] has been adopted. In the Voucher Data, any extensions are listed in a list Attribute named 'extensions'. In JSON serialization, these extensions each require a unique name, and therefore this name MUST be allocated by IANA. The name MUST be the same as the YANG extension module name. The 'extensions' list Attribute allows for new standard extensions to be defined without changes to the 'ietf-voucher' YANG module. Items within that list are either strings (in JSON serialization), or integers (in CBOR serialization using SIDs); both are always defined in the entries of the Voucher Extensions Registry (see Section 11.5).

Extensions are full YANG modules, which are subject to the SID allocation process described in [RFC9254]. When an extension is serialized, the extension is placed in a sub-map in the value of a new key/value pair in the 'voucher' container element. In JSON serialization, the corresponding key is the name of the extension, prefixed by the string "extension:". In CBOR serialization, the corresponding key is the SID which is allocated as the YANG extension module SID. This will typically require the absolute SID value Tag(47) to be applied to this key (see Section 4.2.1 of [RFC9254] or the final example in Section 7.2).

Note that this differs from the mechanism described in [RFC8520]: there, a sub-map is not used. Instead, keys are created by combining the module name and the Attribute as a string, as a result of using the YANG "augment" mechanism. The [RFC8520] mechanism uses more bytes, but is also not easily translatable to CBOR.

As the Voucher Request YANG module is created by YANG augment of the Voucher YANG module, any extension defined for the Voucher is also valid for a Voucher Request.

7.6. Manufacturer Private Extensions

A manufacturer might need to communicate content in the Voucher (or in the Voucher Request), which are never subject to standardization. While they can use the Voucher extensions mechanism defined in Section 7.5, it does require allocation of a SID value in order to do minimal-sized encoding in case of CBOR Voucher Data. Note that [RFC9254] does not strictly require use of SIDs: instead of a SID value, the full string name can always be used. But this would significantly increase the size of the Voucher Data.

Instead, a manufacturer MAY use the 'manufacturer-private' Attribute to put any content they wish. In CBOR serialization, if a plain CBOR map would be used, it would be subject to delta encoding: so use of this Attribute requires that the contents are bstr-encoded [CBOR] [RFC8949], Section 3.1 (Major type 2). In JSON serialization, delta encoding does not get in the way, and the manufacturer MAY use any encoding that is convenient for them, but base64URL encoding [RFC4648], Section 5 is RECOMMENDED.

8. Voucher Request Artifact

[BRSKI], Section 3 defined a "voucher-request" Artifact as an augmented Artifact from the "voucher" Artifact originally defined in [RFC8366]. That definition has been moved to this document, and translated from the "yang-data" extension [RFC8040] to the "sx:structure" extension [RFC8791].

8.1. Tree Diagram

The following tree diagram illustrates a high-level view of a Voucher Request document. The notation used in this diagram is described in [RFC8340]. Each node in the diagram is fully described by the YANG module in Section 8.2.

```
module: ietf-voucher-request
```

```

structure voucher:
  +-- created-on?          yang:date-and-time
  +-- extensions*          union
  +-- manufacturer-private? binary
  +-- assertion?           enumeration
  +-- serial-number        string
  +-- idevid-issuer?       binary
  +-- pinned-domain-cert?  binary
  +-- pinned-domain-pubk?  binary
  +-- pinned-domain-pubk-sha256? binary
  +-- domain-cert-revocation-checks? boolean
  +-- last-renewal-date?   yang:date-and-time
  +-- expires-on?         yang:date-and-time
  +-- nonce?              binary
  +-- est-domain?         ietf:uri
  +-- additional-configuration-url? ietf:uri
  +-- prior-signed-voucher-request? binary
  +-- proximity-registrar-cert?  binary
  +-- proximity-registrar-pubk?  binary
  +-- proximity-registrar-pubk-sha256? binary
  +-- agent-signed-data?    binary
  +-- agent-provided-proximity-registrar-cert? binary
  +-- agent-sign-cert?     binary

```

8.2. "ietf-voucher-request" Module

The 'ietf-voucher-request' YANG module is derived from the 'ietf-voucher' module.

```

<CODE BEGINS> file "ietf-voucher-request@2023-01-10.yang"
module ietf-voucher-request {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:ietf-voucher-request";
  prefix vcr;

  import ietf-yang-structure-ext {
    prefix sx;
  }
  import ietf-voucher {
    prefix vch;
  }
  description
    "This module defines the format for a Voucher,
    which is produced by a Pledge's manufacturer or
    delegate (MASA) to securely assign a Pledge to
    an 'Owner', so that the Pledge may establish a secure
    connection to the Owner's network infrastructure";

```

```
reference
  "RFC XXXX: A Voucher Artifact for
    Bootstrapping Protocols";
}

organization
  "IETF ANIMA Working Group";
contact
  "WG Web:    <https://datatracker.ietf.org/wg/anima/>
  WG List:    <mailto:anima@ietf.org>
  Author:     Kent Watsen
               <mailto:kent+ietf@watsen.net>
  Author:     Michael Richardson
               <mailto:mcr+ietf@sandelman.ca>
  Author:     Max Pritikin
               <mailto:pritikin@cisco.com>
  Author:     Toerless Eckert
               <mailto:tte@cs.fau.de>
  Author:     Qiufang Ma
               <mailto:maqiufang1@huawei.com>
  Author:     Esko Dijk
               <mailto:esko.dijk@iotconsultancy.nl>";
description
  "This module defines the format for a Voucher Request.
  It is a superset of the Voucher itself.
  It provides content to the MASA for consideration
  during a voucher request procedure and subsequent
  Voucher creation.

  Copyright (c) 2023 IETF Trust and the persons identified as
  authors of the code. All rights reserved.

  Redistribution and use in source and binary forms, with or
  without modification, is permitted pursuant to, and subject to
  the license terms contained in, the Revised BSD License set
  forth in Section 4.c of the IETF Trust's Legal Provisions
  Relating to IETF Documents
  (https://trustee.ietf.org/license-info).

  This version of this YANG module is part of RFC XXXX
  (https://www.rfc-editor.org/info/rfcXXXX); see the RFC itself
  for full legal notices.

  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 (RFC 2119) (RFC 8174) when, and only when,
  they appear in all capitals, as shown here.";
```

```
// RFCEDITOR: please replace XXXX in this entire code fragment
// with the RFC number assigned and remove this notice.

revision 2023-01-10 {
  description
    "Updates and additions described by RFC XXXX";
  reference
    "RFC XXXX: A Voucher Artifact for Bootstrapping Protocols";
}
revision 2021-05-20 {
  description
    "Initial version";
  reference
    "RFC 8995: Bootstrapping Remote Secure Key Infrastructure
    (BRSKI)";
}

grouping voucher-request-grouping {
  description
    "Grouping to allow reuse/extensions in future work.";
  uses vch:voucher-artifact-grouping {
    refine "last-renewal-date" {
      description
        "A last-renewal-date field
        is not valid in a voucher request, and
        any occurrence MUST be ignored";
    }
    refine "domain-cert-revocation-checks" {
      description
        "The domain-cert-revocation-checks field
        is not valid in a voucher request, and
        any occurrence MUST be ignored";
    }
    refine "assertion" {
      description
        "Any assertion included in registrar voucher
        requests SHOULD be ignored by the MASA.";
    }
  }
}
leaf prior-signed-voucher-request {
  type binary;
  description
    "If it is necessary to change a voucher, or re-sign and
    forward a voucher request that was previously provided
    along a protocol path, then the previously signed
    voucher SHOULD be included in this field.

    For example, a pledge might sign a voucher request
```

with a proximity-registrar-cert, and the registrar then includes it as the prior-signed-voucher-request field. This is a simple mechanism for a chain of trusted parties to change a voucher request, while maintaining the prior signature information.

The Registrar and MASA MAY examine the prior signed voucher information for the purposes of policy decisions. The MASA SHOULD remove all prior-signed-voucher-request information when signing a voucher for imprinting so as to minimize the final voucher size.";

```
}
leaf proximity-registrar-cert {
  type binary;
  description
    "An X.509 v3 certificate structure as specified by
    RFC 5280, Section 4 encoded using the ASN.1
    distinguished encoding rules (DER), as specified
    in [ITU.X690.1994].

    The first certificate in the Registrar TLS server
    certificate_list sequence (the end-entity TLS
    certificate, see [RFC8446]) presented by the Registrar
    to the Pledge.
    This MUST be populated in a Pledge's voucher request
    when a proximity assertion is requested.";
}
leaf proximity-registrar-pubk {
  type binary;
  description
    "The proximity-registrar-pubk replaces
    the proximity-registrar-cert in constrained uses of
    the voucher-request.
    The proximity-registrar-pubk is the
    Raw Public Key of the Registrar. This field is encoded
    as specified in RFC7250, section 3.
    The ECDSA algorithm MUST be supported.
    The EdDSA algorithm as specified in
    draft-ietf-tls-rfc4492bis-17 SHOULD be supported.
    Support for the DSA algorithm is not recommended.
    Support for the RSA algorithm is a MAY, but due to
    size is discouraged.";
}
leaf proximity-registrar-pubk-sha256 {
  type binary;
  description
    "The proximity-registrar-pubk-sha256
```

is an alternative to both proximity-registrar-pubk and pinned-domain-cert. In many cases the public key of the domain has already been transmitted during the key agreement protocol, and it is wasteful to transmit the public key another two times.

The use of a hash of public key info, at 32-bytes for sha256 is a significant savings compared to an RSA public key, but is only a minor savings compared to a 256-bit ECDSA public-key.

Algorithm agility is provided by extensions to this specification which may define a new leaf for another hash type.";

```
}
leaf agent-signed-data {
  type binary;
  description
    "The agent-signed-data field contains a data artifact
    provided by the Registrar-Agent to the Pledge for
    inclusion into the voucher request.

    This artifact is signed by the Registrar-Agent and contains
    data, which can be verified by the pledge and the registrar.
    This data contains the pledge's serial-number and a
    created-on information of the agent-signed-data.

    The format is intentionally defined as binary to allow
    the document using this leaf to determine the encoding.";
}
leaf agent-provided-proximity-registrar-cert {
  type binary;
  description
    "An X.509 v3 certificate structure, as specified by
    RFC 5280, Section 4, encoded using the ASN.1
    distinguished encoding rules (DER), as specified
    in ITU X.690.
    The first certificate in the registrar TLS server
    certificate_list sequence (the end-entity TLS
    certificate; see RFC 8446) presented by the
    registrar to the registrar-agent and provided to
    the pledge.
    This MUST be populated in a pledge's voucher-request
    when an agent-proximity assertion is requested.";
  reference
    "ITU X.690: Information Technology - ASN.1 encoding
    rules: Specification of Basic Encoding Rules (BER),
    Canonical Encoding Rules (CER) and Distinguished
    Encoding Rules (DER)
```

```

    RFC 5280: Internet X.509 Public Key Infrastructure
    Certificate and Certificate Revocation List (CRL)
    Profile
    RFC 8446: The Transport Layer Security (TLS)
    Protocol Version 1.3";
}
leaf agent-sign-cert {
    type binary;
    description
        "An X.509 v3 certificate structure, as specified by
        RFC 5280, Section 4, encoded using the ASN.1
        distinguished encoding rules (DER), as specified
        in ITU X.690.
        This certificate can be used by the pledge,
        the registrar, and the MASA to verify the signature
        of agent-signed-data. It is an optional component
        for the pledge-voucher request.
        This MUST be populated in a registrar's
        voucher-request when an agent-proximity assertion
        is requested.";
    reference
        "ITU X.690: Information Technology - ASN.1 encoding
        rules: Specification of Basic Encoding Rules (BER),
        Canonical Encoding Rules (CER) and Distinguished
        Encoding Rules (DER)
        RFC 5280: Internet X.509 Public Key Infrastructure
        Certificate and Certificate Revocation List (CRL)
        Profile";
}
}

// Top-level statement: called "voucher" to match RFC8995
sx:structure voucher {
    uses voucher-request-grouping;
}
}
<CODE ENDS>
```

8.3. ietf-voucher-request SID values

[RFC9254] explains how to serialize YANG into CBOR, and for this a series of SID values are required. The below SID values are assigned to the 'ietf-voucher-request' YANG module elements and are considered normative.

The right column shows the XPath expression for the YANG data node to which the SID value is assigned. In the XPath, the ellipsis (...) notation is used to abbreviate the structure path '/ietf-voucher-request:voucher' to let each entry fit on one line.

SID	Assigned to
2500	module ietf-voucher-request
2501	data /ietf-voucher-request:voucher
2502	data ../assertion
2503	data ../created-on
2504	data ../domain-cert-revocation-checks
2505	data ../expires-on
2506	data ../idevid-issuer
2507	data ../last-renewal-date
2508	data ../nonce
2509	data ../pinned-domain-cert
2510	data ../prior-signed-voucher-request
2511	data ../proximity-registrar-cert
2512	data ../proximity-registrar-pubk-sha256
2513	data ../proximity-registrar-pubk
2514	data ../serial-number
2515	data ../agent-provided-proximity-registrar-cert
2516	data ../agent-sign-cert
2517	data ../agent-signed-data
2518	data ../pinned-domain-pubk
2519	data ../pinned-domain-pubk-sha256
2520	data ../additional-configuration-url
2521	data ../est-domain
2522	data ../extensions
2523	data ../manufacturer-private

The 'assertion' Attribute is an enumerated type, and has values as defined in Table 2.

9. Design Considerations

9.1. Renewals Instead of Revocations

The lifetimes of Vouchers may vary. In some Onboarding protocols, the Vouchers may be created and consumed immediately, whereas in other Onboarding solutions, there may be a significant time delay between when a Voucher is created and when it is consumed. In cases when there is a time delay, there is a need for the Pledge to ensure that the assertions made when the Voucher was created are still valid.

A revocation artifact is generally used to verify the continued validity of an assertion such as a PKIX certificate [RFC5280], web token, or Voucher. With this approach, a potentially long-lived assertion is paired with a reasonably fresh revocation status check to ensure that the assertion is still valid. However, this approach increases solution complexity, as it introduces the need for additional protocols and code paths to distribute and process the revocations.

Addressing the shortcomings of revocations, this document recommends instead the use of lightweight renewals of short-lived non-revocable Vouchers. That is, rather than issue a long-lived Voucher, where the 'expires-on' Attribute is set to some distant date, the expectation is for the MASA to instead issue a short-lived Voucher, where the 'expires-on' Attribute is set to a relatively near date, along with a promise (reflected in the 'last-renewal-date' Attribute) to reissue the Voucher again when needed. Importantly, while issuing the initial Voucher may incur heavyweight verification checks ("Are you who you say you are?" "Does the Pledge actually belong to you?"), reissuing the Voucher should be a lightweight process, as it ostensibly only updates the Voucher's validity period. With this approach, there is only the one Artifact, and only one code path is needed to process it; there is no possibility of a Pledge choosing to skip the revocation status check because, for instance, the OSCP Responder ([RFC5280]) is not reachable.

While this document recommends issuing short-lived Vouchers, the Voucher Artifact does not restrict the ability to create long-lived Vouchers, if required; however, no revocation method is described.

Note that a Voucher may be signed by a chain of intermediate CAs leading up to the trust anchor CA known by the Pledge. Even though the Voucher itself is not revocable, it is still revoked, per se, if one of the intermediate CA certificates is revoked.

9.2. Voucher Per Pledge

The solution described herein originally enabled a single Voucher to apply to many Pledges, using lists of regular expressions to represent ranges of serial numbers. However, it was determined that blocking the renewal of a Voucher that applied to many devices would be excessive when only the ownership for a single Pledge needed to be blocked. Thus, the Voucher format now only supports a single serial number to be listed.

10. Security Considerations

10.1. Clock Sensitivity

An attacker could use an expired Voucher to gain control over a device that has no understanding of time. The device cannot trust NTP as a time reference, as an attacker could control the NTP stream.

There are three things to defend against this: 1) devices are required to verify that the 'expires-on' Attribute has not yet passed, 2) devices without access to time can use nonces to get ephemeral Vouchers, and 3) Vouchers without expiration times may be used, which will appear in the audit log, informing the security decision.

This document defines a Voucher format that contains time values for expirations, which require an accurate clock in order to be processed correctly. Vendors planning on issuing Vouchers with expiration values must ensure that devices have an accurate clock when shipped from manufacturing facilities and take steps to prevent clock tampering. If it is not possible to ensure clock accuracy, then Vouchers with time values for expirations should not be issued.

10.2. Protect MASA Signing Key in HSM

Pursuant to the recommendation made in Section 6.1 for the MASA to be deployed as an online Voucher signing service, it is RECOMMENDED that the MASA's private key used for signing Vouchers is protected by a hardware security module (HSM).

10.3. Test Domain Certificate Validity When Signing

If a Domain certificate is compromised, then any outstanding Vouchers for that Domain could be used by the attacker. In this case, the Domain administrator is clearly expected to initiate revocation of any Domain identity certificates (as is normal in PKIX [RFC5280] solutions).

Similarly, they are expected to contact the MASA to indicate that an outstanding (presumably short lifetime) Voucher should be blocked from automated renewal. Protocols for Voucher distribution are RECOMMENDED to check for revocation of Domain identity certificates before the signing of Vouchers.

10.4. YANG Module Security Considerations

The YANG modules specified in this document define the schema for data that is subsequently encapsulated by secure signed-data structures, such as the CMS signed-data described in Section 6.1. As such, all of the YANG-modeled data is protected from modification.

Implementations should be aware that the signed data is only protected from external modification; the data is still visible. This potential disclosure of information doesn't affect security so much as privacy. In particular, adversaries can glean information such as which devices belong to which organizations and which CRL Distribution Point and/or OCSP Responder URLs are accessed to validate the Vouchers. When privacy is important, the CMS signed-data content type SHOULD be encrypted, either by conveying it via a mutually authenticated secure transport protocol (e.g., TLS [RFC8446]) or by encapsulating the signed-data content type with an enveloped-data content type (Section 6 of [RFC5652]), though details for how to do this are outside the scope of this document.

The use of YANG to define data structures, via the "sx:structure" extension [RFC8791], is relatively new and distinct from the traditional use of YANG to define an API accessed by network management protocols such as NETCONF [RFC6241] and RESTCONF [RFC8040]. For this reason, this security considerations section does not follow the template described by Section 3.7 of [YANG-GUIDE].

11. IANA Considerations

11.1. The IETF XML Registry

This document registers two URIs in the "IETF XML Registry" [RFC3688].

IANA has registered the following:

URI: urn:ietf:params:xml:ns:yang:ietf-voucher
Registrant Contact: The ANIMA WG of the IETF.
XML: N/A, the requested URI is an XML namespace.

This reference should be updated to point to this document.

11.2. The YANG Module Names Registry

This document registers two YANG module in the "YANG Module Names" registry [RFC6020].

IANA has registered the following:

```
name: ietf-voucher
namespace: urn:ietf:params:xml:ns:yang:ietf-voucher
prefix: vch
reference: RFC 8366
```

This reference should be updated to point to this document.

11.3. The Media Types Registry

IANA has registered the media type: application/voucher-cms+json, and this registration should be updated to point to this document.

11.4. The SMI Security for S/MIME CMS Content Type Registry

IANA has registered the OID 1.2.840.113549.1.9.16.1.40, 'id-ct-animaJSONVoucher'. This registration should be updated to point to this document.

11.5. The Voucher Extensions Registry

IANA is asked to create a registry of Voucher extensions as follows:

```
Registry name: Voucher Extensions Registry
Registry policy: First Come First Served
Reference: an optional document
Extension name: UTF-8-encoded string, not to exceed 40
                characters.
Extension SID: the YANG module SID value that defines the
                extension per Section 7.5.
```

Each extension MUST follow the rules specified in this specification. As is usual, the IANA issues early allocations in accordance with [RFC7120].

Note that the SID module value is allocated as part of a [CORESID] process. This may be from a SID range managed by IANA, or from any other MegaRange. Future work may allow for PEN based allocations. IANA does not need to separately allocate a SID value for this column.

Extension name strings for standards track documents are single words, given by the YANG Module Name. They do not contain dots. For vendor proprietary extensions, the string SHOULD be made unique by putting the extension name in the form a fully-qualified domain name (FQDN) [RFC3696], such as "fuubar.example.com"

Vendor proprietary extensions do not need to be registered with IANA, but vendors MAY do so.

Designated Experts should review for standards track documents for clarity, but the process is essentially tied to WG and IESG process: There are no choices in the extension names (which is always the YANG module name), or SID value (which is from another IANA process). For non-standards track extensions, the Designated Expert should review whatever document is provided, if any. The stability of the reference may be of concern. The Designated Expert should determine if the work overlaps with existing efforts; and if so suggest merging. However, as registration is optional, the Designated Expert should not block any registrations.

12. References

12.1. 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/rfc/rfc8995>>.
- [CBOR] Internet Standard 94,
<<https://www.rfc-editor.org/info/std94>>.
At the time of writing, this STD comprises the following:
- 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>>.
- [cBRSKI] Richardson, M., Van der Stok, P., Kampanakis, P., and E. Dijk, "Constrained Bootstrapping Remote Secure Key Infrastructure (cBRSKI)", Work in Progress, Internet-Draft, draft-ietf-anima-constrained-voucher-29, 18 October 2025, <<https://datatracker.ietf.org/doc/html/draft-ietf-anima-constrained-voucher-29>>.
- [CLOUD] Friel, O., Shekh-Yusef, R., and M. Richardson, "Bootstrapping Remote Secure Key Infrastructure (BRSKI) Cloud Registrar", Work in Progress, Internet-Draft, draft-ietf-anima-brski-cloud-19, 9 September 2025, <<https://datatracker.ietf.org/doc/html/draft-ietf-anima-brski-cloud-19>>.

- [CORESID] Veillette, M., Ed., Pelov, A., Ed., Petrov, I., Ed., Bormann, C., and M. Richardson, "YANG Schema Item Identifier (YANG SID)", RFC 9595, DOI 10.17487/RFC9595, July 2024, <<https://www.rfc-editor.org/rfc/rfc9595>>.
- [IDEVID] IEEE Standard, "IEEE 802.1AR Secure Device Identifier", 2018, <<https://1.ieee802.org/security/802-1ar/>>.
- [ITU-T.X690.2015] International Telecommunication Union, "Information Technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)", ITU-T Recommendation X.690, ISO/IEC 8825-1, August 2015, <<https://www.itu.int/rec/T-REC-X.690/>>.
- [jBRSKI] Werner, T. and M. Richardson, "JWS signed Voucher Artifacts for Bootstrapping Protocols", Work in Progress, Internet-Draft, draft-ietf-anima-jws-voucher-16, 15 January 2025, <<https://datatracker.ietf.org/doc/html/draft-ietf-anima-jws-voucher-16>>.
- [PRM] Fries, S., Werner, T., Lear, E., and M. Richardson, "BRSKI with Pledge in Responder Mode (BRSKI-PRM)", Work in Progress, Internet-Draft, draft-ietf-anima-brski-prm-23, 3 June 2025, <<https://datatracker.ietf.org/doc/html/draft-ietf-anima-brski-prm-23>>.
- [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/rfc/rfc2119>>.
- [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/rfc/rfc5280>>.
- [RFC5652] Housley, R., "Cryptographic Message Syntax (CMS)", STD 70, RFC 5652, DOI 10.17487/RFC5652, September 2009, <<https://www.rfc-editor.org/rfc/rfc5652>>.
- [RFC6020] Bjorklund, M., Ed., "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", RFC 6020, DOI 10.17487/RFC6020, October 2010, <<https://www.rfc-editor.org/rfc/rfc6020>>.

- [RFC7120] Cotton, M., "Early IANA Allocation of Standards Track Code Points", BCP 100, RFC 7120, DOI 10.17487/RFC7120, January 2014, <<https://www.rfc-editor.org/rfc/rfc7120>>.
- [RFC7950] Bjorklund, M., Ed., "The YANG 1.1 Data Modeling Language", RFC 7950, DOI 10.17487/RFC7950, August 2016, <<https://www.rfc-editor.org/rfc/rfc7950>>.
- [RFC7951] Lhotka, L., "JSON Encoding of Data Modeled with YANG", RFC 7951, DOI 10.17487/RFC7951, August 2016, <<https://www.rfc-editor.org/rfc/rfc7951>>.
- [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/rfc/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/rfc/rfc8259>>.
- [RFC8791] Bierman, A., Bjorklund, M., and K. Watsen, "YANG Data Structure Extensions", RFC 8791, DOI 10.17487/RFC8791, June 2020, <<https://www.rfc-editor.org/rfc/rfc8791>>.
- [RFC9254] Veillette, M., Ed., Petrov, I., Ed., Pelov, A., Bormann, C., and M. Richardson, "Encoding of Data Modeled with YANG in the Concise Binary Object Representation (CBOR)", RFC 9254, DOI 10.17487/RFC9254, July 2022, <<https://www.rfc-editor.org/rfc/rfc9254>>.
- [ZERO-TOUCH] 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/rfc/rfc8572>>.

12.2. Informative References

- [COSE] Internet Standard 96, <<https://www.rfc-editor.org/info/std96>>. At the time of writing, this STD comprises the following:
- Schaad, J., "CBOR Object Signing and Encryption (COSE): Structures and Process", STD 96, RFC 9052, DOI 10.17487/RFC9052, August 2022, <<https://www.rfc-editor.org/info/rfc9052>>.

Schaad, J., "CBOR Object Signing and Encryption (COSE): Countersignatures", STD 96, RFC 9338, DOI 10.17487/RFC9338, December 2022, <<https://www.rfc-editor.org/info/rfc9338>>.

[fairhair] Open Connectivity Foundation, "Fairhair Specification", 1 November 2019, <<https://openconnectivity.org/developer/specifications/fairhair/>>.

[I-D.ietf-lake-authz]
Selander, G., Mattsson, J. P., Vuini, M., Fedrecheski, G., and M. Richardson, "Lightweight Authorization using Ephemeral Diffie-Hellman Over COSE (ELA)", Work in Progress, Internet-Draft, draft-ietf-lake-authz-06, 20 October 2025, <<https://datatracker.ietf.org/doc/html/draft-ietf-lake-authz-06>>.

[I-D.vangeest-lamps-cms-euf-cma-signeddata]
Van Geest, D. and F. Strenzke, "Best Practices for CMS SignedData with Regards to Signed Attributes", Work in Progress, Internet-Draft, draft-vangeest-lamps-cms-euf-cma-signeddata-02, 20 October 2025, <<https://datatracker.ietf.org/doc/html/draft-vangeest-lamps-cms-euf-cma-signeddata-02>>.

[imprinting]
Wikipedia, "Wikipedia article: Imprinting (psychology)", 1 October 2025, <[https://en.wikipedia.org/w/index.php?title=Imprinting_\(psychology\)&oldid=1314466188](https://en.wikipedia.org/w/index.php?title=Imprinting_(psychology)&oldid=1314466188)>.

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

[RFC3688] Mealling, M., "The IETF XML Registry", BCP 81, RFC 3688, DOI 10.17487/RFC3688, January 2004, <<https://www.rfc-editor.org/rfc/rfc3688>>.

[RFC3696] Klensin, J., "Application Techniques for Checking and Transformation of Names", RFC 3696, DOI 10.17487/RFC3696, February 2004, <<https://www.rfc-editor.org/rfc/rfc3696>>.

[RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, DOI 10.17487/RFC4648, October 2006, <<https://www.rfc-editor.org/rfc/rfc4648>>.

- [RFC6125] Saint-Andre, P. and J. Hodges, "Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)", RFC 6125, DOI 10.17487/RFC6125, March 2011, <<https://www.rfc-editor.org/rfc/rfc6125>>.
- [RFC6241] Enns, R., Ed., Bjorklund, M., Ed., Schoenwaelder, J., Ed., and A. Bierman, Ed., "Network Configuration Protocol (NETCONF)", RFC 6241, DOI 10.17487/RFC6241, June 2011, <<https://www.rfc-editor.org/rfc/rfc6241>>.
- [RFC7435] Dukhovni, V., "Opportunistic Security: Some Protection Most of the Time", RFC 7435, DOI 10.17487/RFC7435, December 2014, <<https://www.rfc-editor.org/rfc/rfc7435>>.
- [RFC8040] Bierman, A., Bjorklund, M., and K. Watsen, "RESTCONF Protocol", RFC 8040, DOI 10.17487/RFC8040, January 2017, <<https://www.rfc-editor.org/rfc/rfc8040>>.
- [RFC8340] Bjorklund, M. and L. Berger, Ed., "YANG Tree Diagrams", BCP 215, RFC 8340, DOI 10.17487/RFC8340, March 2018, <<https://www.rfc-editor.org/rfc/rfc8340>>.
- [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/rfc/rfc8366>>.
- [RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <<https://www.rfc-editor.org/rfc/rfc8446>>.
- [RFC8520] Lear, E., Droms, R., and D. Romascanu, "Manufacturer Usage Description Specification", RFC 8520, DOI 10.17487/RFC8520, March 2019, <<https://www.rfc-editor.org/rfc/rfc8520>>.
- [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/rfc/rfc8792>>.
- [RFC9110] Fielding, R., Ed., Nottingham, M., Ed., and J. Reschke, Ed., "HTTP Semantics", STD 97, RFC 9110, DOI 10.17487/RFC9110, June 2022, <<https://www.rfc-editor.org/rfc/rfc9110>>.

- [RFC9499] Hoffman, P. and K. Fujiwara, "DNS Terminology", BCP 219, RFC 9499, DOI 10.17487/RFC9499, March 2024, <<https://www.rfc-editor.org/rfc/rfc9499>>.
- [RFC9525] Saint-Andre, P. and R. Salz, "Service Identity in TLS", RFC 9525, DOI 10.17487/RFC9525, November 2023, <<https://www.rfc-editor.org/rfc/rfc9525>>.
- [SECUREJOIN]
Richardson, M., "6tisch Zero-Touch Secure Join protocol", Work in Progress, Internet-Draft, draft-ietf-6tisch-dtsecurity-zerotouch-join-04, 8 July 2019, <<https://datatracker.ietf.org/doc/html/draft-ietf-6tisch-dtsecurity-zerotouch-join-04>>.
- [Stajano99theresurrecting]
Stajano, F. and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad-Hoc Wireless Networks", 1999, <<http://www.cl.cam.ac.uk/research/dtg/www/files/publications/public/files/tr.1999.2.pdf>>.
- [YANG-GUIDE]
Bierman, A., "Guidelines for Authors and Reviewers of Documents Containing YANG Data Models", BCP 216, RFC 8407, DOI 10.17487/RFC8407, October 2018, <<https://www.rfc-editor.org/rfc/rfc8407>>.

Appendix A. Examples

A.1. Key pairs associated with examples

The following Voucher Request has been produced using the IDevID [IDEVID] public (certificate) and private key. They are included so that other developers can match the same output.

The private RSA key:

```
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIIBHNh6r8QRevRuo+tEmBJeFjQKf6bpFA/9NGoltv+9sNoAoGCCqGSM49
AwEHoUQDQgAEA6NlQ4ezfMAKmoecrfb0OBMc1AyEH+BATkF58FsTSyBxs0SbSWLx
FjDOuwB9gLGn2TsTUMJ6VPw5Z/TP4hJw==
-----END EC PRIVATE KEY-----
```

The IDevID certificate (public key):

-----BEGIN CERTIFICATE-----

MIIBrzCCATWgAwIBAgIEHxj+5zAKBggqhkJOPQQDAjAmMSQwIgYDVQQDDDBtoawDo
d2F5LXRlc3QuZXhhbXBsZS5jb20gQ0EwIBcNMjEwNDI3MTgyOTMwWhgPMjk5OTEy
MzEwMDAwMDBaMBwxGjAYBgNVBAUTETAwLUQwLUU1LUYyLTAwLTAYMFkwEwYHkoZI
zj0CAQYIKoZIZj0DAQcDQgAEANlQ4ezfMAKmoecrfb0OBMc1AyEH+BATkF58FsT
SyBxs0SbSWLxFjDOuwB9gLGn2TsTUJumJ6VPw5Z/TP4hJ6NZMFcwHQYDVR0OBBYE
FEWizJaWAGQ3sLojZWRkVAgGbFatMAKGA1UdEwQCMAAwKwYIKwYBBQUHASEHxYd
aGlnaHdheS10ZXN0LmV4YW1wbGUuY29tOjk0NDMwCgYIKoZIZj0EAWIDAaAAwZQIw
YirbvjT3G8uf3iaOQwD5DYjId6jdPAhAVLzSPbbccCvDf8oZIZqgq8VRjqrFnt6L
AjeASl1Z+Efh7QOXqMDHqIH6qIbtZ2Q3UXpunKOCTW2tvPM1np1qom1/fyUcA+/w
uptx

-----END CERTIFICATE-----

The Certification Authority that created the IDevID:

===== NOTE: '\ ' line wrapping per RFC 8792 =====

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 1016146354 (0x3c9129b2)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN = highway-test.example.com CA

Validity

Not Before: Apr 5 19:36:57 2021 GMT

Not After : May 6 05:36:57 2021 GMT

Subject: CN = highway-test.example.com CA

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (3072 bit)

Modulus:

00:b4:7b:27:42:49:9f:ed:85:47:74:ff:f6:50:cd:
5d:22:1a:64:38:22:f8:09:d2:d6:f3:60:d8:98:7f:
e5:84:52:1e:d9:ce:96:b4:dc:a6:43:74:67:27:d9:
9d:42:7d:bf:1a:43:92:9b:d1:dd:34:9b:41:d2:e3:
d5:59:b3:40:fc:b3:c9:e1:58:84:3f:87:f7:06:45:
25:26:4c:bf:a1:45:72:a0:0a:5b:86:41:d7:8e:be:
d3:38:b5:aa:66:69:bd:3a:fd:e9:b5:b8:a2:79:c4:
f0:a5:3c:9e:91:94:32:1e:9c:b0:7f:25:46:5b:76:
1d:86:23:85:b0:62:45:5c:a8:6f:fb:c5:26:e1:dd:
a8:f2:68:ab:c5:8c:b4:58:b4:2e:96:49:fa:fe:d2:
ea:a5:11:68:c2:8d:f4:58:ab:30:bd:dd:1b:29:97:
00:18:6f:59:40:9c:3a:2a:e4:96:25:bb:12:f4:1a:
11:72:6d:31:f6:b4:e1:cc:d8:9a:0c:aa:a8:aa:a4:
64:e3:f1:06:1c:c0:09:df:62:ba:04:cb:70:b0:c4:
f7:ca:35:22:ea:a9:c7:52:e1:ce:27:fb:6c:52:39:
b7:22:b3:5d:97:cb:0a:9f:75:a3:af:16:ef:e6:b2:
1b:6a:c3:0b:1d:15:fd:b8:d8:e7:8a:f6:f4:99:1c:

```
23:97:4b:80:e9:79:a3:85:16:f8:dd:bd:77:ef:3a:
3c:8e:e7:75:56:67:36:3a:dd:42:7b:84:2f:64:2f:
13:0e:fa:b0:3b:11:13:7e:ae:78:a6:2f:46:dd:4b:
11:88:e4:7b:19:ab:21:2d:1f:34:ba:61:cd:51:84:
a5:ec:6a:c1:90:20:70:e3:aa:f4:01:fd:0c:6e:cd:
04:47:99:31:70:79:6c:af:41:78:c1:04:2a:43:78:
84:8a:fe:c3:3d:f2:41:c8:2a:a1:10:e0:b7:b4:4f:
4e:e6:26:79:ac:49:64:cf:57:1e:2e:e3:2f:58:bd:
6f:30:00:67:d7:8b:d6:13:60:bf
```

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints: critical

CA:TRUE

X509v3 Key Usage: critical

Certificate Sign, CRL Sign

X509v3 Subject Key Identifier:

33:12:45:B7:1B:10:BE:F3:CB:64:E5:4C:50:80:7C:9D:88:\
65:74:40

X509v3 Authority Key Identifier:

33:12:45:B7:1B:10:BE:F3:CB:64:E5:4C:50:80:7C:9D:88:\
65:74:40

Signature Algorithm: sha256WithRSAEncryption

Signature Value:

```
05:37:28:85:37:39:71:87:ec:5c:f0:51:19:55:4a:b7:e0:2a:
e6:61:30:d4:e2:2b:ad:7a:db:12:fc:8a:a6:6e:15:82:80:10:
fa:5d:67:60:e8:54:14:e3:89:d6:4e:60:89:98:5b:ab:fe:32:
26:aa:02:35:68:4e:c6:2e:ce:08:36:d1:ea:a0:97:3d:76:38:
6e:9d:4b:6f:33:d2:fa:c2:7e:b0:59:bc:75:97:17:d1:1b:c5:
c4:58:ae:7b:7e:87:e5:87:2b:8b:6b:10:16:70:7c:c8:65:c7:
d0:62:5d:f3:b5:06:af:03:8b:32:dd:88:f0:07:2b:5d:61:58:
61:35:54:a6:ce:95:81:a2:6e:fa:b5:aa:25:e1:41:53:9d:e7:
4b:7e:93:88:79:6b:dd:a3:6e:9a:0d:bd:85:b4:2d:66:b9:cc:
01:13:f1:b5:d5:91:cc:86:5e:a7:c8:4a:8f:4d:9d:f8:17:31:
32:7d:50:d5:c2:79:a0:41:a0:69:83:33:16:14:35:26:10:3b:
23:eb:60:d9:28:68:99:d5:55:61:89:b5:35:5d:8b:fe:b1:96:
32:69:3e:8b:c2:a2:4e:e1:d8:76:04:3c:87:91:5d:66:9e:81:
a5:bf:18:2e:3e:39:da:4f:68:57:46:d2:1d:aa:81:51:3b:33:
72:da:e9:7d:12:b6:a1:fc:c7:1d:c1:9c:bd:92:e8:1b:d2:06:
e8:0b:82:2a:4f:23:5a:7a:fa:7b:86:a0:d7:c1:46:e7:04:47:
77:11:cd:da:7c:50:32:d2:6f:fd:1e:0a:df:cf:b1:20:d2:86:
ce:40:5a:27:61:49:2f:71:f5:04:ac:eb:c6:03:70:a4:70:13:
4a:af:41:35:83:dc:55:c0:29:7f:12:4f:d0:f1:bb:f7:61:4a:
9f:8d:61:b0:5e:89:46:49:e3:27:8b:42:82:5e:af:14:d5:d9:
91:69:3d:af:11:70:5b:a3:92:3b:e3:c8:2a:a4:38:e5:88:f2:
6f:09:f4:e5:04:3b
```

-----BEGIN CERTIFICATE-----

MIIELTCCApWgAwIBAgIEPJepsjANBgkqhkiG9w0BAQsFADAmMSQwIgYDVQQDDDBto
aWdod2F5LXRlc3QuZXhhbXBsZS5jb20gQ0EwHhcNMjEwNDA1MTkzNjU3WhcNMjEw

NTA2MDUzNjU3WjAmMSQwIgYDVQQDDBtoaWdod2F5LXRlc3QuZXhhbXBsZS5jb20g
Q0EwggGiMA0GCSqGSIb3DQEBAQUAA4IBjwAwggGKAoIBgQC0eydCSZ/thUd0//ZQ
zV0iGmQ4IvgJ0tbzYNIYf+WEUh7Zzpa03KZDdGcn2Z1Cfb8aQ5Kb0d00m0HS49VZ
s0D8s8nhWlQ/h/cGRSUmTL+hRXKgCluGQdeOvtM4tapmab06/emluKJ5xPClPJ6R
lDIenLB/JUZbdh2GI4WwYkVcqG/7xSbh3ajyaKvFjLRYtC6WSfr+0uqlEWjCjfrY
qzC93RsplwAYb1lAnDoq5JYluxL0GhFybTH2tOHM2JoMqqiqpGTj8QYcwAnfYroE
y3CwXPfKNSLqqcdS4c4n+2xSObcisl2XywqfdaOvFu/mshtqwwsdFf2420eK9vSZ
HCOXS4DpeaOFFvjdvXfvOjyO53VWZzY63UJ7hC9kLxMO+rA7ERN+rnimL0bdSxGI
5HsZqyEtHzS6YclRhKXsasGQIHDjqvQB/QxuzQRHmTFweWyvQXjBBCpDeISK/sM9
8kHIKqEQ4Le0T07mJnmsSWTPVx4u4y9YvW8wAGfXi9YTYL8CAwEAAANjMGewDwYD
VR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFDMSRbcbEL7z
y2TlTFCAfJ2IZXRAMB8GA1UdIwQYMBaAFDMSRbcbEL7zy2TlTFCAfJ2IZXRAMA0G
CSqGSIb3DQEBCwUAA4IBgQAFNyifNzlxh+xc8FEZVUq34CrmYTDU4iutetsS/Iqm
bhWCgBD6XWdg6FQU44nWTmCJmFur/jImqgIlaE7GLs4INtHqoJc9djhunUtvM9L6
wn6wWbx1lxfRG8XEWK57f0flhyuLaxAWcHzIZcfQYl3ztQavA4sy3YjwBytdYVhh
NVSmzpWBom76taol4UFTnedLfpOIeWvdo26aDb2FtC1mucwBE/G11ZHMh16nyEqP
TZ34FzEyfVDVwnmgQaBpgzMWFDUmEDSj62DZKGiZlVVhibU1XYv+sZYyaT6LwqJO
4dh2BDyHkVlmmoGlvxguPjnaT2hXRtIdqoFROzNy2ul9Erah/McdwZy9kugb0gbo
C4IqTyNaevp7hqDXwUbnBED3Ec3afFay0m/9Hgrfz7Eg0obOQFonYUkvcfUErOvG
A3CkcBNKr0Elg9xVwCl/Ek/Q8bv3YUqfjWGwXolGSeMni0KCXq8UldmRaT2vEXBb
o5I748gqpDjliPJvCfTlBDs=
-----END CERTIFICATE-----

The private key for the Certification Authority that created the
IDeVID:

-----BEGIN RSA PRIVATE KEY-----

MIIG5AIBAACKAYEAtHsnQkmf7YVHdP/2UMldIhpkOCL4CdLW82DYmH/lhFie2c6W
tNymQ3RnJ9mdQn2/GkOSm9HdNjTB0uPVWbNA/LPJ4ViEP4f3BkUlJky/oUVyoApb
hkHXjr7TOLWqZmm9Ov3ptbiiecTwpTyekZQyHpywfyVGW3YdhiOFsGJFXKhv+8Um
4d2o8mirxYy0WLQulkn6/tLqpRFowo30WKswvd0bKZcAGG9ZQJw6KuSWJbsS9BoR
cm0x9rThzNiaDKqoqqRk4/EGHMAJ32K6BMtwsMT3yUi6qnHUuHOJ/tsUjm3IrNd
l8sKn3Wjrxbv5rIbasMLHRX9uNjnivb0mRwj10uA6Xmjhrb43b137zo8jud1Vmc2
Ot1Ce4QvZC8TDvqwOxETfq54pi9G3UsRiOR7GashLR80umHNUYSl7GrBkCBw46r0
Af0Mbs0ER5kxchlsr0F4wQQqQ3iEiv7DPfJBByCqhEOC3tE905iZ5rElkz1ceLuMv
WLlvMABn14vWE2C/AgMBAAECggGAAUF6HHP2sOhkfuPpCtbi9wHIALv9jdPxuu/J
kgYRysHnhQxy7/85C08eaKCS/4twcPZXZs4nA96wro73RRCCOz/k/7Rl9yszBNAM
WgXer3iU05jW2jBLF6ssPRDGhr/lmSt7HNCUENTV99BcKhcl4iCk+b2Ap9JCklRc
8cU9Rk/Ft7K/eoLYUhd4Wn+IibXfPRx2qp89Erj0SaZDNPq79BY9wiRS09iyfkiX
/wRoJwsOLrSfunQYD0dlSs+XAs+NKeKmB6chmPhP+sYTXx+zFj+36NRjq2dxkYSH
hb9peJ5yzTDhLQpagV5D36VXQsqHawvgEu6cQAfcZ4Iqmnura7zyBysfk4YzzizO
rsc9rYGP10U05W0EpKR/IcNfMGwtDbHe1/7z+0JSVDe/ldht8YrwX3ogd5rNbhlf
lUE+D7rof8E8g6Uz4TWI8dpMDaXCzjgz6q2iiW770R5xCphLFbuNh/SnbkYNYNEo
k8AN+Fx+w3EO7Cg4aaETB76iNXVBAoHBAOibavF4IYurjni39Z/6vIhO3lF7VdNj
x9gz9Om6MmZNFsBUB8PLyoQEYI46ygf8TO/BSfiHyUMncohmXWsoUXiFZV412aVqk
HgZg+MWSKuYuTmGk/CouYQzd7RtrLl8TpPncXhsJIZ48ppcVGnMhNWZmTLj/Kqf6
oDfsI7QhZy8fUxgIJ3vWoC5zFeQYzXpID4PKkn6mXczt6YiQHFJuvqVjpf1Vh9WZ
leIhCBxoI76jluU3ZiOEWFkmsWddIPyIwKBwQDGobnHJl1IJeny/KaHBVt8OECV
wEH6lAxp4jcxYgQCbPVGJzNs+BstjoiY+UDrG2MVyJ+dj+yS2lfDBJcyzo/mE/ox
0odGpKJ9MVk4Mb4m543Jllgb9ZQmJmKzJipqpRetmXV22QB0sJyaYL4M3zroqwl7
tEf6HH1vmc9XQwACJOrlm+k4ldjutwmuCE2JYoNbLdcrCgdf006Z3bhNknbrFD
OrB40xxlH5u38kDU7ifieQ4jvUEWk6a5+sIR+rUCgcEAyp+AJEJyblmObShKhgaE
LvUN4cvfcppL3rqVtvhkqOrizwXVsryadhE4GjjztsAJiYpCp820hJl2d3Z6NuhR
KxnJg8gvdC7cnM/iRUd5wzN5QePXaeMm1W+I+UZ/iYDySFmnfEOTDmVkn9N0EQknS
2f2pPcnBXbybzrscSvCCEvFlj9yikGTg+jV0TlMvwyJ8qWBQBpVjxn1E3poyobgo
yKeqUC0qe24ju2zssNoOsSXF7x3c976BWi5ec/UTJAjAoHAYZ+GwRzTwqPvsZ7+
8Yluh0TWaUNOqistVrT5z2m08uo+OjZ2De563Q5OGzEV+PdC4afy2uurqBlr3Mta
zHu9OaVD6EzCc7PisIkagoXgIRrZEuSzdTpjj8R56fauDjAjZSaJFtpcYP2UWkOF
5KmqOEQpokzeu0xZUgPUXlzmIEu2Z6hJ2/i6KBJP6GRCh7C1INZJywMp39siC7y
sBlf83qQYK5toVSQvffe/skvl/dc3vAERQh0/vWekfVugIupAoHBAJj9U/aFU/c5
Kc/94hmer6TljinMSn0EI9nlJ5FkY2BDmzgeAD9/kNBbPHRjIyMa5Ow7rH04Lt09
U837yytEcBmErNzMuBhOX+nirXXq1Dp5LMNkHP3gnPy0XC2Cu5m2vH/qbFhIlRER
lGXCxBrWOzovXFu090oIjOhwCbxt7GWZH/GMUUJGXJb+s1CzQNz1qiXKng7XpluA
S9jVch5pKqmWvDYyRbXmmCe9Ju0RnBCgOIuGUICPjEFay+myLdgQ0A==

-----END RSA PRIVATE KEY-----

The MASA certificate that signs the Voucher:

```
-----BEGIN CERTIFICATE-----
MIIBcDCB9qADAgECAGQLhwoxMAoGCCqGSM49BAMCMCYxJDAiBgNVBAMMG2hpZ2h3
YXktdGVzdC5leGFtcGxlLmNvbSBDQTAeFw0yMTA0MTMyMTQwMTZaFw0yMzA0MTMy
MTQwMTZaMCgxJjAkBgNVBAMMHWhpZ2h3YXktdGVzdC5leGFtcGxlLmNvbSBNQVNB
MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEqgQVo0S54kT4yfkBxumdhOcHrps
qbOpMKmiMln3oB1HAW25MJV+gqi4tMFfSJ0iEwt8kszfWXX4rLgJS2mnpaMQMA4w
DAYDVR0TAQH/BAIwADAKBggqhkJOPQDAGNpADBMAjEArsthLdRcjW6GqgsGHcbT
YLoyczYl0yOFSYcczpQjeRqeQVUkHRUioUi7CsCrPBNzAjEAhjxns5Wi4uX5rfkd
nME0Mnjlz+rVRwOfAL/QWctRwpgEgSSKURNQsXWYL52otPS5
-----END CERTIFICATE-----
```

The private key for MASA certificate signs the Voucher:

```
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIFhdd0eDdzip67kXx72K+KHGJQYJHNY8pkiLJ6CcvxMGoAoGCCqGSM49
AwEHoUQDQgAEqgQVo0S54kT4yfkBxumdhOcHrpsqbOpMKmiMln3oB1HAW25MJV+
gqi4tMFfSJ0iEwt8kszfWXX4rLgJS2mnpQ==
-----END EC PRIVATE KEY-----
```

A.2. Example CMS-signed Voucher Request

MIIGjQYJKoZIhvcNAQcCoIIIGfjCCBnoCAQExDTALBglghkgBZQMEAgEwggO1
BgkqhkiG9w0BBWGGggOWBIIDknsiaWV0Zi12b3VjaGVyLXJlcXVlc3Q6dm91
Y2hlciI6eyJhc3NlcnRpb24iOiJwcm94aW1pdHkiLCJjcmVhdGVkLW9uIjoi
MjAyMi0wNy0xMFQxNzowODoxOC41OTgtMDQ6MDAiLCJzZXJpYWwtbnVtYmVy
IjoiMDAtRDAtRTUtRjItMDAtMDIiLCJub25jZSI6IjR2VHNwcmFMyQ2VxQnpv
RWRvaWZNMmciLCJwcm94aW1pdHktdmVnaXN0cmFyLWNlcnQiOiJNSU1DRURD
Q0FaYwBd0lCQWdJRvLGYTZAveFLQmdncWhrak9QUVFEQWpCde1SSXdfQVlL
Q1pJbWlaUhlMR1FCR1JZQ1kyRXhHVEFYQmdvSmtYUprL0lzWkFFWkZnbHpZ
VzVrWld4dFlXNHhQREE2QmdOVkBJBTU1NMlp2ZFclMF1XbHVMWFJsYzNRdVpY
aGhiWEJzWlMlamIyMGdWVzV6ZEhKMWJtY2dSbTkxYm5SaGFXNGdVbTl2ZENC
RFFUQWVGdZB5TVRFeElqUXhPVFF6TURWYUZ3Mh1NekV4TWpReE9UUXpNRFZh
TUZNeEvqQVFCZ29Ka2lhSmsvSXNaQUVaRmdKallURVpNQmNHQ2dtU0pvbVQ4
aXhrQVJrV0NYTmhibVJsYkcxagJqRWlNQ0FHQTfVRUF3d1pabTkxYm5SaGFX
NHRkR1Z6ZEM1bGVHRnRjR3hstG1OdmJUQ1pNQk1HqnlxR1NNND1BZ0VHQ0Nx
R1NNND1Bd0VIQTBJQUJKWmxVSEkwdXAvbDNlWmY5dkNCYitsSW5vRU1FZ2M3
Um8rWFpDdGpBSTBDRDFmSmZKU19oSX15RG1IV3lZaU5GYlJDSdlmeWFyZmt6
Z1g0cDB6VG16cWpQake4TUNvR0ExVWRKUUVCL3dRZ01CNEddQ3NHQVfVRkJ3
TWNcZ2dyQmdFRkRJRy0RBZ1lJS3dZQkRJVUhbD0V3RGdZRFZSMFBBUUGvQkFR
REFnZUFNQW9HQ0NxR1NNND1CQU1DQdTJnQU1HVUNNUUNkU1pSSjgzTU5SQ3ph
Myt2T0JhMDFoNHfadjJss2hkK0RmaEI0WURodkdwaldvbFplSEh3TmI3QXRC
Q010Y1V3Q01Ib054b21rK3hXN0F0MWhYRWhwMy9NY1hpQWR6blpicFZxK3hK
RVppaFhVMzZJQmp2WWdXREY5aXZxeEppwRGJ5dz09In19oIIBszCCAa8wggE1
oAMCAQICBB8Y/ucwCgYIKoZIzj0EAwIwJjEkMCIGA1UEAwbaGlnaHdheS10
ZXN0LmV4YW1wbGUuY29tIENBMCAxDTIxMDQyNzE4MjkzMFoYDzi5OTkxMjMx
MDAwMDAwWjAcMRowGAYDVQQFEExEwMC1EMC1FNS1GMi0wMC0wMjBZMBMGByqG
SM49AgEGCCqGSM49AwEHA0IABAOjdUOHs3zACpQHnK329DgTHNQMHb/gQE5B
efBbE0sgcbNEM0li8RYwzrsAfYCXp9k7E1Cbpielt8OWf0z+ISejWTBxMB0G
AlUdDgQWBBRFiMyWlgBkN7C6I2VkZFQIBmxWrtAJBgNVHRMEAjaAMCsGCCsG
AQUFBwEgBB8WHWhpZ2h3YXktdGVzdC5leGFtcGxlLmNvbTo5NDQzMAoGCCqG
SM49BAMCA2gAMGUcmGIIQ27409xvLhd4mjkMA+Q2IyHeo3TwIQFS87D223HAr
w3/KGSGaoKvFUY6q3zbeiwIxALJdWfhHx+0Dl6jAx6iB+qiG7WdkN1F6bpyj
gkltrbzzNZ6daqJtf38lHAPv8LqbcTGCAQQwggEAAgEBMC4wJjEkMCIGA1UE
AwbaGlnaHdheS10ZXN0LmV4YW1wbGUuY29tIENBAgQfGP7nMAsGCWCGSAFl
AwQCAaBpMBGCSqGSIb3DQEJAzELBgkqhkiG9w0BBWewHAYJKoZIhvcNAQKF
MQ8XDTIyMDcxMDIxMDgxOFowLWYJKoZIhvcNAQkEMSIEIFc4jo6OnilTLkM/
fcc9p5au4ANjvJvJRXsAKK6+RcTvMAoGCCqGSM49BAMCBEcwRQIhAOjoOdgh
Sr+Hk2r2APsfsl+QJba0uRf/+zXA70yb6mRCAiB9aS6Wj8kBCWEvvfsDue41
KW00ukOBQxdPGpJqg+GAMw==

A.3. Example CMS-signed Voucher from MASA

MIIGPQYJKoZIhvcNAQcCoIIIGLjCCBioCAQExDTALBglghkgBZQMEAgEwgGOU
BgkqhkiG9w0BBWGgggOFBIIDgXsiaWV0Zi12b3VjaGVyOnZvdWNoZXIiOnsi
YXNzZXJ0aW9uIjoibG9nZ2VkiIwiY3JlYXRlZC1vbiI6IjIwMjItMDctMTBU
MTc6MDg6MTguNzIwLTA0OjAwIiwic2VyaWFsLW51bWJlciI6IjAwLUQwLUU1
LUYyLTAwLTAYIiwibm9uY2UiOiI0dlRzchBTMkNlcUJ6aEVkb2lmTTJnIiwi
cGlubmVklWRvbWFPbiIjZXJ0IjoitULjQ0VEQ0NBWmFnQXdJQkFnSUVZRM2
WlRBS0JnZ3Foa2pPUFFRREFqQnRNUkl3RUFZS0NaSWlpWlB5TEDRQkdSWUNZ
MkV4R1RBWEJnb0praWFKay9Jc1pBRVpGZ2x6WVclalpXeHRZVzR4UERBNkNjN
TlZCQjU1NTTjJadmRXNTBZV2x1TFhSbGMzUXVaWGhoYlhCc1pTNWpiMjBnVlc1
emRISjFibWNNUm05MWJlUmhhVzRnVW05dmRDQkRRVEFlRncweU1URXhNalF4
TlRReklEVmFGdzB5TXpFeElqUXhPVFF6TURWYU1GTXhFakFRQmdvSmtptYUpr
L0lZwKFFWkZnSmpZVEVaTUJjR0NnbVNkb2lUOG14a0FSaldDWE5oYm1SbGJH
MWhiakVpTUNBR0ExVUVBd3daWm05MWJlUmhhVzR0ZEdWemRDNWxlR0Z0Y0d4
bExtTnZiVEJaTUJNR0J5cUdTTTQ5QWdFR0NDcUdTTTQ5QXdfSEEWsUFCslps
VUHJMhVwL2wzZVpmOXZDQmIrbElub0VNRWdjN1JvK1haQ3RqQUkwQ0QxZkpm
SlIvaEl5eURTsfD5WWlORmJSQ0g5ZnlhcmZremdYNHAWelRpenFqUGpBOElD
b0dBmVvkslFFQi93UWdNqjRHQ0NzR0FRVUZCd01jQmdnckJnRUZCUWNEQWdZ
Sut3WUJCUVVIQXdfD0RnWURWUjBQqVFIL0JBUURBZ2VBTUFvR0NDcUdTTTQ5
QkFNQ0EyZ0FNR1VDTVFDZFNauko4M01OUkN6YTMrdk9CYTAXaDRxWnYybEto
ZCtEZmhCNFlEaHZHcGtXb2xaZUId05iN0F0QkNNdGJVd0NNSG90eG9payt4
VzdBdDFoWEVocDMvTWNyaUFkem5aYnBWcSt4SkVaaWhYVTM2SUJqdlInV0RG
OWl2cXhKcERieXc9PSJ9faCCAXQwggFwMIH2oAMCAQICBAuHCjEwCgYIKoZI
zj0EAwIwJjEkMCIGA1UEAwbaGlnaHdheS10ZXN0LmV4YWlwbGUuY29tIENB
MB4XDTIxMDQxMzIxNDAXNloXDTIzMDQxMzIxNDAXNlowKDEmMCQGA1UEAwwd
aGlnaHdheS10ZXN0LmV4YWlwbGUuY29tIE1BU0EwWTATBgqhkiJOPQIBBggq
hkjOPQMBBwNCAASqBBWjRLniRPjJ+RSHG6Z0c5weumyps6kwqaiYwFegHUcB
bbkwlX6CqLi0wV9InSITC3ySzN9ZcrisuAlLaaeloxAwDjAMBGNVHRMBAf8E
AjaAAMAoGCCqGSM49BAMCA2kAMGYCMQCuy2Et1FyNboaqCwYdxtNgujJzNiXT
I4VJhxxZ0lCN5Gp5BVSQdFSKhSLsKwKs8E3MCMQCGPGezlaLi5fmt+R2cwTQy
ePXP6tVHA58Av9BZylHCmASBJIpRElCxdbIvnai09LkxggEEMIIBAAIBATAu
MCYxJDAiBgNVBAMMG2hpZ2h3YXktdGVzdC5leGFtcGxlLmNvbSBDOQQIEC4cK
MTALBglghkgBZQMEAgGgaTAYBgqhkiG9w0BCQMxCwYJKoZIhvcNAQcCBMBwG
CSqGSIB3DQEJBTEPFw0yMjA3MTAyMTA4MThaMC8GCSqGSIB3DQEJBDEiBCBA
77EhoAybh5R6kK89jDefpxRy8Q6rDo1cnlwgvCzXbzAKBggqhkiJOPQQDAgRH
MEUCIQD4RnuXwKvYVvwamwVq3VYv7dXcM7bzLg7FXTkhvYqPzwIgXTJxVV5a
cLMARoeHgThS5JU5QA2PJMLGF82UcSNTsEY=

A.4. Example JWS-signed Voucher from MASA

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

```
{
  "payload": "eyJpZXRMZXZvdWNoZXI6dm91Y2hlciI6eyJhc3NlcnRpb24iOiJwcm\
94aWlpdHkiLCJzZXJpYWwtbnVtYmVyIjoIY2FmZmUtOTg3NDUiLCJub25jZSI6IjYyYT\
JlNzY5M2Q4MmZjZGEyNjI0ZGUlOGZiNjcyMmU1IiwIY3JlYXRlZC1vbiI6IjIwMjU0MT\
AtMTVUMDA6MDA6MDBaIiwicGlubmVklWRvbWVpbiIjZXJ0IjoITU1JQmd6Q0NBU3FnQX\
dJQkFnSUdBV09XZTBsrklBb0dDQ3FHU000OUJBTUNNRfV4RXpBUkJnTlZCQW9NQ2sxNV\
FuVnphVzVsYzNNeERUQUxCZ05WQkFjTUJGTnBkRlV4RHpbTkJnTlZCQU1NQmxSbGMzUk\
RRVEFlRncweE9EQTFNaV3T0RRM016QmFGdzB5T0RBMU1qVXdPRFEzTXpCYU1EVXhFek\
FSQmdOVkjbB01DazElUW5WemFXNWxjM014RFRBTEJnTlZCQWNNQkZ0cGRHVXhEekFOQm\
dOVkjbTUlCbFJsYzNSRFFUQ1pNQk1HQnlxR1NNND1BZ0VHQ0Nxr1NNND1Bd0VIQTBjQU\
JIOUVCdXVXVjdJS09ya040YjdsYTU1b2J5dFduV1p3Rm5QdHVSMdlhd3dVSEZQZStOWW\
M1WjVwdUo2ZEFuK0FrVzFnY1poQ1hWR0JBM0crSXlSVlVXU2pKakFrTUJJR0ExVWRfD0\
VCL3dRSU1BUWJBZjhdQVFBd0RnWURWUjBQOVFIL0JBUURBZ01FTUFvR0NDcUdTTTQ5Qk\
FNQ0EwY0FNRVFSURlWlc2SWZjeUsvLzBBVFk2S21NYjRNMFFJU1FTZFVGvjdQNZlLWV\
ZJWVVBaUJRMVYrd0xSM1Uzd2NjWnhHSE1ISGx0N2M3ZzFDaFdNRVkvEfoU1NZawlnPT\
0ifX0",
  "signatures": [
    {
      "protected": "eyJ4NWMiOlSiTU1JQmNEQ0I5cUFEQWdFQ0FnUUxod294TUFv\
R0NDcUdTTTQ5QkFNQ01DWXhKREFpQmdOVkjbTUlHMmhwWjJoM1lYa3RkRlZ6ZEM1bGVH\
RnRjR3hstG1OdmJtQkRRVEFlRncweU1UQTBVNE15TVRRd01UWmFGdzB5TXpBME1UTXlN\
VFF3TVRaYU1DZ3hKakFrQmdOVkjbTUlIV2hwWjJoM1lYa3RkRlZ6ZEM1bGVHRnRjR3hs\
TG1OdmJtQk5RVk5CTUZrd0V3WUhlb1pJemowQ0FRWU1Lb1pJemowREFRY0RRZ0FFcWdR\
Vm8wUzU0a1Q0eWZrYk1J4dW1kSE9jSHJwc3FiT3BNS21pTWxuM29CMUhbVzI1TUWk2dx\
aTR0TUZmU0owaUV3dDhrc3pmV1hLNHJMZ0pTmmlucGFNUU1BNHdEQVlEVlIwVEFRSC9C\
QU13QURBS0JnZ3Foa2pPUFFRREFnTnBBREJtQWpFQXJzdGhmZfJjalC2R3Fnc0dIY2JU\
WUxveWN6WWweU9GU1ljY3pwUWplUnFlUVZVa0hSVWlvVWk3Q3NDclBCTnpBakVBaGp4\
bnM1V2k0dVglcmZrZG5NRTBNbmoxeityVlJ3T2ZBTC9RV2N0UndwZ0VnU1NLVWJOUXNY\
V3lMNTJvdFBTNSJdLCJ0eXAiOiIj2b3VjaGVyLWp3cytqc29uIiwIYXNjaXNjaXNjaXN\
fQ",
      "signature": "s_gJM_4qzzlboxDtqh6Ybip42J_0_Y4CMdrMFb8lpPsAhDHVR\
AESNRL3n6M_F8dGQHmlfu66x83cK9E5cPtEdag"
    }
  ]
}
```

Figure 1: Example JWS Voucher

Acknowledgements

The authors would like to thank the following people for lively discussions on list and in the halls (ordered by last name): William Atwood, Michael H. Behringer, Steffen Fries, Sheng Jiang, Thomas Werner.

Max Pritikin and Kent Watsen were instrumental in creating the original [RFC8366].

Authors' Addresses

Kent Watsen
Watsen Networks
Email: kent+ietf@watsen.net

Michael C. Richardson (editor)
Sandelman Software
Email: mcr+ietf@sandelman.ca, <https://orcid.org/0000-0002-0773-8388>
URI: <http://www.sandelman.ca/>

Esko Dijk
IoTconsultancy.nl
Email: esko.dijk@iotconsultancy.nl

Max Pritikin
Cisco Systems
Email: pritikin@cisco.com

Toerless Eckert
Futurewei Technologies Inc.
2330 Central Expy
Santa Clara, 95050
United States of America
Email: tte@cs.fau.de

Qiufang Ma
Huawei
101 Software Avenue, Yuhua District
Nanjing
210012
China
Email: maqiufang1@huawei.com