6tisch Working Group
Internet-Draft
Intended status: Informational
Expires: June 14, 2018

M. Richardson
Sandelman Software Works

December 11, 2017

Constrained Voucher Profile for Bootstrapping Protocols
draft-richardson-anima-ace-constrained-voucher-00

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 builds upon the work in [I-D.ietf-anima-voucher], encoding the resulting artifact in CBOR. Use with two signature technologies are described.

Additionally, this document explains how constrained vouchers may be transported in the [I-D.vanderstok-ace-coap-est] protocol.

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 June 14, 2018.

Table of Contents

1. Introduction

Enrollment of new nodes into constrained networks with constrained nodes present unique challenges.

There are bandwidth and code space issues to contend. A solution such as [I-D.ietf-anima-bootstrapping-keyinfra] may be too large in terms of code space or bandwidth required.

This document defines a constrained version of [I-D.ietf-anima-voucher]. Rather than serializing the YANG definition in JSON, it is serialized into CBOR ([RFC7049]).

This document follows a similar, but not identical structure as [I-D.ietf-anima-voucher]. Some sections are left out entirely.

The CBOR definitions for this constrained voucher format are defined using the mechanism describe in [I-D.ietf-core-yang-cbor] using the SID mechanism explained in [I-D.ietf-core-sid]. As the tooling to convert YANG documents into an list of SID keys is still in its infancy, the table of SID values presented here should be considered normative rather than the output of the pyang tool.

Two methods of signing the resulting CBOR object are described in this document. One is CMS [RFC5652]. The other is COSE [RFC8152] signatures.

2. Terminology

The following terms are defined in [I-D.ietf-anima-voucher], and are used identically as in that document: artifact, imprint, domain, Join Registrar/Coordinator (JRC), Manufacturer Authorized Signing Authority (MASA), pledge, Trust of First Use (TOFU), and Voucher.

3. Requirements Language

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in BCP 14, RFC 2119 [RFC2119] and indicate requirement levels for compliant STuPiD implementations.

4. Survey of Voucher Types

[I-D.ietf-anima-voucher] provides for vouchers that assert proximity, that authenticate the registrar and that include different amounts of anti-replay protection.

This document does not make any extensions to the types of vouchers.

Time based vouchers are included in this definition, but given that constrained devices are extremely unlikely to know the correct time, their use is very unlikely. Most users of these constrained vouchers

will be online and will use live nonces to provide anti-replay protection.

[I-D.ietf-anima-voucher] defined only the voucher artifact, and not the Voucher Request artifact, which was defined in [I-D.ietf-anima-bootstrapping-keyinfra].

This document defines both a constrained voucher and a constrained voucher-request. They are presented in the order voucher-request, followed by voucher response as this is the time order that they occur.

5. Artifacts

This section describes the abstract (tree) definition as explained in [I-D.ietf-netmod-yang-tree-diagrams] first. This provides a high-level view of the contents of each artifact.

Then the assigned SID values are presented. These have been assigned using the rules in [I-D.ietf-core-yang-cbor], with an allocation that was made via the http://comi.space service. ((EDNOTE: it is unclear if there is further IANA work))

5.1. Voucher Request artifact

5.1.1. Tree Diagram

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

  grouping voucher-request-cwt-grouping
    +---- voucher
       +---- created-on
       |       yang:date-and-time
       +---- expires-on?
       |       yang:date-and-time
       +---- assertion
       |       enumeration
       +---- serial-number                                  string
       +---- idevid-issuer?                                 binary
       +---- pinned-domain-cert                             binary
       +---- domain-cert-revocation-checks?                 boolean
       +---- nonce?                                         binary
       +---- last-renewal-date?
       |       yang:date-and-time
       +---- proximity-registrar-subject-public-key-info?   binary
```

5.1.2. SID values

5.1.3. YANG Module

```
<CODE BEGINS> file "ietf-cwt-voucher-request.yang"
/* -*- c -*- */
module ietf-cwt-voucher-request {
  yang-version 1.1;

  namespace
    "urn:ietf:params:xml:ns:yang:ietf-cwt-voucher-request";
  prefix "vcwt";

  import ietf-voucher {
    prefix "v";
  }

  organization
   "IETF 6tisch Working Group";

  contact
   "WG Web:   <http://tools.ietf.org/wg/6tisch/>
    WG List:  <mailto:6tisch@ietf.org>
    Author:   Michael Richardson
              <mailto:mcr+ietf@sandelman.ca>";

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

    This version provides a very restricted subset appropriate
    for very constrained devices.
    In particular, it assumes that nonce-ful operation is
    always required, that expiration dates are rather weak, as no
    clocks can be assumed, and that the Registrar is identified
    by a pinned Raw Public Key.

    The key words 'MUST', 'MUST NOT', 'REQUIRED', 'SHALL', 'SHALL NOT',
    'SHOULD', 'SHOULD NOT', 'RECOMMENDED', 'MAY', and 'OPTIONAL' in
    the module text are to be interpreted as described in RFC 2119.";

  revision "YYYY-MM-DD" {
    description
     "Initial version";
    reference
```

```
     "RFC XXXX: Voucher Profile for Constrained Devices";
  }

  // Grouping defined for future usage
  grouping voucher-request-cwt-grouping {
    description
      "Grouping to allow reuse/extensions in future work.";

    uses v:voucher-artifact-grouping {
      augment "voucher" {
        description "Base the CWT voucher-request upon the regular one";
        leaf proximity-registrar-subject-public-key-info {
          type binary;
          description
            "The proximity-registrar-subject-public-key-info replaces
         the proximit-registrar-cert in constrained uses of
         the voucher-request.
         The proximity-registrar-subject-public-key-info 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.";
        }
      }
    }
  }
}
<CODE ENDS>
```

5.1.4. Example voucher request artifacts

TBD

5.2. 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 that is a CBOR encoded instance of the YANG module defined in Section 5.3 that has been signed with CMS or with COSE.

5.3. Tree Diagram

```
   module: ietf-cwt-voucher

     grouping voucher-cwt-grouping
       +---- voucher
          +---- created-on
          |       yang:date-and-time
          +---- expires-on?
          |       yang:date-and-time
          +---- assertion                                enumeration
          +---- serial-number                            string
          +---- idevid-issuer?                           binary
          +---- pinned-domain-cert                       binary
          +---- domain-cert-revocation-checks?           boolean
          +---- nonce?                                   binary
          +---- last-renewal-date?
          |       yang:date-and-time
          +---- pinned-domain-subject-public-key-info?   binary
```

5.4. SID values

```
        SID Assigned to
   --------- --------------------------------------------------
     1001100 module ietf-cwt-voucher
     1001101 module ietf-restconf
     1001102 module ietf-voucher
     1001103 module ietf-yang-types
     1001104 data .../ietf-cwt-voucher:voucher
     1001105 data .../assertion
     1001106 data .../created-on
     1001107 data .../domain-cert-revocation-checks
     1001108 data .../expires-on
     1001109 data .../idevid-issuer
     1001110 data .../last-renewal-date
     1001111 data .../nonce
     1001112 data .../pinned-domain-cert
     1001113 data .../pinned-domain-subject-public-key-info
     1001114 data .../serial-number
          No .sid file
```

5.5. YANG Module

```
<CODE BEGINS> file "ietf-cwt-voucher.yang"
/* -*- c -*- */
module ietf-cwt-voucher {
  yang-version 1.1;
```

```
   namespace
     "urn:ietf:params:xml:ns:yang:ietf-cwt-voucher";
   prefix "vcwt";

   import ietf-voucher {
     prefix "v";
   }

   organization
    "IETF 6tisch Working Group";

   contact
    "WG Web:   <http://tools.ietf.org/wg/6tisch/>
     WG List:  <mailto:6tisch@ietf.org>
     Author:   Michael Richardson
               <mailto:mcr+ietf@sandelman.ca>";

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

     This version provides a very restricted subset appropriate
     for very constrained devices.
     In particular, it assumes that nonce-ful operation is
     always required, that expiration dates are rather weak, as no
     clocks can be assumed, and that the Registrar is identified
     by a pinned Raw Public Key.

     The key words 'MUST', 'MUST NOT', 'REQUIRED', 'SHALL', 'SHALL NOT',
     'SHOULD', 'SHOULD NOT', 'RECOMMENDED', 'MAY', and 'OPTIONAL' in
     the module text are to be interpreted as described in RFC 2119.";

   revision "YYYY-MM-DD" {
     description
      "Initial version";
     reference
      "RFC XXXX: Voucher Profile for Constrained Devices";
   }

   // Grouping defined for future usage
   grouping voucher-cwt-grouping {
     description
       "Grouping to allow reuse/extensions in future work.";

     uses v:voucher-artifact-grouping {
       augment "voucher" {
```

```
         description "Base the CWT voucher upon the regular one";
         leaf pinned-domain-subject-public-key-info {
           type binary;
           description
             "The pinned-domain-subject replaces the
          pinned-domain-certificate in constrained uses of
          the voucher.  The pinned-domain-public-key-info 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.";
         }
       }
     }
   }
 }
 <CODE ENDS>
```

5.5.1. Example voucher artifacts

TBD

5.6. CMS format voucher and voucher-request artifacts

5.7. COSE format voucher and voucher-request artifacts

6. Design Considerations

6.1. Renewals instead of Revocations

6.2. Voucher Per Pledge

7. Security Considerations

7.1. Clock Sensitivity

Protect Voucher PKI in HSM ## Test Domain Certificate Validity when Signing

8. IANA Considerations

8.1. The IETF XML Registry

This document registers two URIs in the IETF XML registry [RFC3688]. Following the format in [RFC3688], the following registration is requested:

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

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

8.2. The YANG Module Names Registry

This document registers two YANG modules in the YANG Module Names registry [RFC6020]. Following the format defined in [RFC6020], the the following registration is requested:

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

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

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

This document registers an OID in the "SMI Security for S/MIME CMS Content Type" registry (1.2.840.113549.1.9.16.1), with the value:

Decimal	Description	References
TBD1	id-ct-animaCBORVoucher	[ThisRFC]

XXX: should a seperate value be used for Voucher Requests?

8.4. The SID registry

The SID range 1001100 was allocated by comi.space to the IETF-CWT-VOUCHER yang module.

The SID range 1001150 was allocated by comi.space to the IETF-CWT-VOUCHER-REQUEST yang module.

EDNOTE: it is unclear if there is further IANA work required.

9. Acknowledgements

TBD

10. References

10.1. Normative References

[I-D.ietf-ace-cbor-web-token]
Jones, M., Wahlstroem, E., Erdtman, S., and H. Tschofenig, "CBOR Web Token (CWT)", draft-ietf-ace-cbor-web-token-09 (work in progress), October 2017.

[I-D.ietf-anima-bootstrapping-keyinfra]
Pritikin, M., Richardson, M., Behringer, M., Bjarnason, S., and K. Watsen, "Bootstrapping Remote Secure Key Infrastructures (BRSKI)", draft-ietf-anima-bootstrapping-keyinfra-09 (work in progress), October 2017.

[I-D.ietf-anima-voucher]
Watsen, K., Richardson, M., Pritikin, M., and T. Eckert, "Voucher Profile for Bootstrapping Protocols", draft-ietf-anima-voucher-06 (work in progress), October 2017.

[I-D.ietf-core-object-security]
Selander, G., Mattsson, J., Palombini, F., and L. Seitz, "Object Security for Constrained RESTful Environments (OSCORE)", draft-ietf-core-object-security-07 (work in progress), November 2017.

[I-D.ietf-core-sid]
Veillette, M. and A. Pelov, "YANG Schema Item iDentifier (SID)", draft-ietf-core-sid-03 (work in progress), December 2017.

[I-D.ietf-core-yang-cbor]
Veillette, M., Pelov, A., Somaraju, A., Turner, R., and A. Minaburo, "CBOR Encoding of Data Modeled with YANG", draft-ietf-core-yang-cbor-05 (work in progress), August 2017.

[I-D.vanderstok-ace-coap-est]
Kumar, S., Stok, P., Kampanakis, P., Furuhed, M., and S. Raza, "EST over secure CoAP (EST-coaps)", draft-vanderstok-ace-coap-est-02 (work in progress), June 2017.

[ieee802-1AR]
IEEE Standard, ., "IEEE 802.1AR Secure Device Identifier", 2009, <http://standards.ieee.org/findstds/standard/802.1AR-2009.html>.

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

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

[RFC7049] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", RFC 7049, DOI 10.17487/RFC7049, October 2013, <https://www.rfc-editor.org/info/rfc7049>.

[RFC7250] Wouters, P., Ed., Tschofenig, H., Ed., Gilmore, J., Weiler, S., and T. Kivinen, "Using Raw Public Keys in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", RFC 7250, DOI 10.17487/RFC7250, June 2014, <https://www.rfc-editor.org/info/rfc7250>.

[RFC8152] Schaad, J., "CBOR Object Signing and Encryption (COSE)", RFC 8152, DOI 10.17487/RFC8152, July 2017, <https://www.rfc-editor.org/info/rfc8152>.

10.2. Informative References

[duckling]
Stajano, F. and R. Anderson, "The resurrecting duckling: security issues for ad-hoc wireless networks", 1999, <https://www.cl.cam.ac.uk/~fms27/papers/1999-StajanoAnd-duckling.pdf>.

[I-D.ietf-netmod-yang-tree-diagrams]
Bjorklund, M. and L. Berger, "YANG Tree Diagrams", draft-ietf-netmod-yang-tree-diagrams-02 (work in progress), October 2017.

[pledge] Dictionary.com, ., "Dictionary.com Unabridged", 2015, <http://dictionary.reference.com/browse/pledge>.

Author's Address

Michael Richardson
Sandelman Software Works

Email: mcr+ietf@sandelman.ca