Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 23, 2019

E. Lear
O. Friel
Cisco Systems

October 20, 2018

Proof of Possession to Devices for Onboarding
draft-lear-brski-pop-00

Abstract

This memo specifies a RESTful interface for local deployments to demonstrate proof of possession to a device or to a manufacturer authorized signing authority (MASA). This covers the case where a MASA would not otherwise have knowledge of where a device is deployed, or when a MASA may not be required. Such knowledge is important to onboard certain classes of devices, such as those on IEEE 802.11 networks.

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 April 23, 2019.

Table of Contents

1. Introduction

[I-D.ietf-anima-bootstrapping-keyinfra] (BRSKI) specifies a means to provision credentials to be used as credentials to operationally access networks. In the initial model, the manufacturer authorized signing authority is assumed to either have knowledge of whether a device is intended to be provisioned on a particular network, or to be able to simply sign all requests. The necessary knowledge to handle the first case is not always easy to come by, and particularly useful to have when a device is trying to determine which network to join, when there is a choice. Such is the case with IEEE 802.11 networks, for example.

Absent that knowledge, should a MASA automatically issue a voucher, the device may onboard to the first BRSKI-aware network, which may well be the wrong one.

In addition, some manufacturers may prefer not to require the existence of a MASA. In these circumstances proof of possession to the device is required.

This memo specifies a RESTful request that devices and registrars employ as an alternative to [I-D.ietf-anima-bootstrapping-keyinfra], in which two additional optional objects may be specified. Three new objects are defined:

1. A simple binary claim that registrar administrator knows this device to belong on the particular deployment network. This object should be conveyed from the registrar to the MASA.

2. A cryptographic claim as such. This would typically be some sort of scanned label or information received as part of a bill of materials that contains some signed evidence of delivery of the

end device to the deployment. This option may be conveyed from the register to the MASA, or when the MASA needn't be contacted, to the device.

3. A statement indicating that the MASA server needn't be contacted at all, and that the device will accept a certificate with the cryptographic claim specified in this memo. This permits offline registration.

Note that this interface is optional. There may well be cases where a MASA already has sufficient knowledge to onboard a device to the correct network. Particularly where the manufacturer requires online registration, when such integration exists, the mechanisms defined in this memo SHOULD NOT be used, as they would be superfluous.

When this model is used, in order to avoid any interoperability problems, a new RESTful endpoint is defined as follows:

"/.well-known/est/request-voucher-with-possession"

The new endpoint is handled precisely as described in Section 5.2 of [I-D.ietf-anima-bootstrapping-keyinfra], with the exception voucher is formed as described below in Section 2.

If the device has indicated that the MASA server needn't be contacted, then the registrar may generate an unsigned voucher response. However, in this case, the registrar must include a valid claim object that has been hashed with an 8-32 bit nonce, immediately succeeded by a non-NULL-terminated key that is provided in UTF8 format. The response MUST be a voucher-brski-pop-request-artifact rather than a voucher-artifact.

2. The Yang Model

```
<CODE BEGINS>file "ietf-brski-possession@2018-10-11.yang"
module ietf-brski-possession {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:ietf-brski-possession";
  prefix mr;

  import ietf-restconf {
    prefix rc;
    description
      "This import statement is only present to access
       the yang-data extension defined in RFC 8040.";
    reference "RFC 8040: RESTCONF Protocol";
  }
  import ietf-voucher {
```

```
    prefix v;
    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
        conn ection to the owner's network infrastructure";

    reference "RFC 8366: Voucher Profile for Bootstrapping Protocols";
  }

  import ietf-voucher-request {
    prefix rv;
    description
      "Voucher request is what we will augment";
    reference "draft-ietf-anima-bootstrapping-keyinfra";
  }

  organization
    "TBD";
  contact
    "Author: Eliot Lear
             <mailto:lear@cisco.com>";
  description
    "This module to provide additional information about
     how a device may be claimed by a particular deployment.
     The owner is asserting that this information has not merely
     been gleaned  directly in-band from the device,
     but rather he or she can confirm ownership independently.

     Copyright (c) 2018 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 Simplified BSD License set forth in Section
     4.c of the IETF Trust's Legal Provisions Relating to IETF Documents
     (http://trustee.ietf.org/license-info).

     This version of this YANG module is part of RFC XXXX; see the RFC
     itself for full legal notices.";

  revision 2018-10-11 {
    description
      "Initial version";
    reference "RFC XXXX: Proof of possession for BRSKI";
  }
  rc:yang-data voucher-brski-pop-request-artifact {
    uses rv:voucher-request-grouping {
```

```
      augment "voucher" {
        description
          "trying to add one more thing into this voucher.";
        leaf out-of-band-claim {
          when 'not(../no-masa-required) and not(../possession-claim)';
          type binary;
          description
            "If this value is true, then the adminsitrator of the
             registrar is claiming that the device being claimed
             has been purchased or otherwise acquired for this
             deployment, and that the information has not merely
             been automatically gleaned directly from the device.";
        }
        leaf possession-claim {
          when 'not(../no-masa-required) and not(../out-of-band-claim)';
          type string;
          description
            "In the context of a voucher-request, this node contains
             a naked key that the MASA will validate.  If valid, the
             MASA will sign a voucher.  The form of this key is left
             to the manufacturer, and is opaque to the registrar";
        }
        leaf no-masa-required {
          when 'not(../possession-claim)and not(../out-of-band-claim)';
          type binary;
          description
            "If true, then the device will not bother to validate
             the provisional TLS connection, but instead assume it
             to be valid.  Only the pledge may set this value.
             The registrar MUST have included the possession-claim
             object.";
        }
      }
    }
  }
  rc:yang-data voucher-with-pop-artifact {
    uses v:voucher-artifact-grouping {
      refine "voucher/pinned-domain-cert" {
        mandatory false;
        }
      refine "voucher/assertion" {
        mandatory false;
        }
      augment "voucher" {
        description
          "Add leaf node for returning a hashed proof of
          possession.";
```

```
          leaf hashed-proof-of-possession {
            type binary;
            mandatory true;
            description
              "A hash of the provided nonce and a key obtained
               by the registrar.  The format is the nonce followed
               immediately by the key.";
          }

          leaf hash-type {
             type enumeration {
               enum SHA256 {
                 description
                   "The type of hash is SHA256.";
               }
             }
             description
               "If not present, assume SHA256.  Otherwise, whatever
                augmented value is present.  This is for algorithmic
                agility.";
           }
         }
       }
     }
}

<CODE ENDS>
```

3. Examples

TBD.

4. IANA Considerations

The following YANG name space should be registered:

o "urn:ietf:params:xml:ns:yang:ietf-brski-possession"

5. Security Considerations

There will be many.

6. Acknowledgments

None yet.

7. Changes from Earlier Versions

Draft -00:

o Initial revision

8. Normative References

[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-16 (work in progress), June 2018.

Authors' Addresses

Eliot Lear
Cisco Systems
Richtistrasse 7
Wallisellen CH-8304
Switzerland

Phone: +41 44 878 9200
Email: lear@cisco.com

Owen Friel
Cisco Systems
170 W. Tasman Dr.
San Jose, CA 95134
United States

Email: ofriel@cisco.com