Workgroup: ace
Internet-Draft: draft-amsuess-ace-brski-ace-00
Published: 7 July 2023
Intended Status: Standards Track
Expires: 8 January 2024
Authors: C. Amsüss

Provisioning ACE credentials through BRSKI

Abstract

The autonomous onboarding mechanisms defined in ANIMA's voucher artifact and the BRSKI protocol provide a means of onboarding a device (the pledge) onto a PKI managed domain. This document extends the voucher with expressions for onboarding it into a domain managed through ACE.

Discussion Venues

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

Discussion of this document takes place on the Authentication and Authorization for Constrained Environments Working Group mailing list (ace@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/ace/.

Source for this draft and an issue tracker can be found at https://gitlab.com/chrysn/brski-ace.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 8 January 2024.

Table of Contents

1. Introduction

[See abstract.]

The main application pattern considered for this kind of enrollment is [authz]: After basic networking services (possibly link-local when used in combination with CoJP as in Appendix A of [authz]) are available, the pledge initiates EDHOC to the lake-authz.arpa anycast address, sending an encrypted identifier for its MASA (party W) in EAD_1.

1.1. Applicability preconditions

While ACE in general does not constrain the type of tokens used, or how the authorization space is split up, using the extensions of this document introduces additional conditions:

* The key used to authenticate the token is a COSE key, and [CWT] are used as tokens.

  The alternative to this constraint is to declare this a blob of some key; what it is depends would be preconfigured in the RS. While this is the general approach of ACE, the author considers it unsuitable for this particular case where a concrete identifier is assigned and thus should have concrete semantics.

Users of any other key format may use this document as scaffolding for declaring an own YANG leaf instead.

While this does allow symmetric keys in theory (and they are used in ACE, for example in the [ace-oscore]) profile), they should not be used in BRSKI deployments, as the secret key would be shared with the MASA as it signs the voucher. [See also the Open Questions section.]

*The pledge is identified with a single audience value. (More precisely, there is an "aud" claim conveyed in the CWTs that can be checked for equality against a configured value).

This rules out setups in which multiple security systems coinhabit the pledge, are enrolled in a single step to a single AS, but act independently at runtime.

Future iterations of this document may relax this, but will always need to express a condition based on which the pledge will know whether or not it may act on a token.

Using these extensions introduces no constraints on the type of scope values used with tokens. The structure of scope values needs to be agreed between the AS and the RS out of band. Typically, the AS will have configured knowledge of how to generate scope values that match the hard-coded model of the RS's firmware from authorizations of its native model.

2. Voucher extensions

This specification adds two leaf nodes to the voucher artifact defined in Section 6.1 of [_8366bis] [this is currently done in a monkey-sees-monkey-does fashion, rather than having the yang files standalone and using pyang to build the tree as is done in 8366bis]:

```
module: ietf-voucher
  augment voucher:
    +-- ace-as-key?                    binary
    +-- ace-aud?                       string
```

2.1. YANG Module

```
<CODE BEGINS> file "ietf-ace-brski-ace@2023-07-07.yang"


module ietf-ace-brski-ace {
  yang-version 1.1;

  namespace "urn:ietf:params:xml:ns:yang:ietf-ace-brski-ace";

  prefix vch-ace;

  import ietf-voucher {
    prefix vch;
    reference "I-D.ietf-anima-rfc8366bis-07";
  }

  organization
    "IETF ACE (Authentication and Authorization for Constrained Environm
    Working Group";

  contact
    "WG Web:   <http://tools.ietf.org/wg/ace/>
     WG List:  <mailto:ace@ietf.org>

     Editor:   Christian Amsüss
               <mailto:christian@amsuess.com>";

  description
    "This module augments the voucher artifact for bootstrapping
    (onboarding) with mechanisms for onboarding onto ACE (Authentication
    and Authorization for Constrained Environments) Authorization
    Servers.

    Copyright (c) 2019 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 2023-07-07 {
    description
      "Initial revision.";

    reference
```

```
      "I-D.amsuess-ace-brski-ace, Provisioning ACE credentials through
      BRSKI";
  }

  uses "vch:voucher-artifact-grouping" {
    augment "voucher" {
      description
        "Mechanisms for onboarding onto ACE (Authentication and Authoriz
        for Constrained Environments) Authorization Servers";

      leaf ace-as-key {
        type binary;
        description
          "Key(s) held by the ACE Authorization Server by which it
          authenticates (and the Resource Server verifies) tokens.
          It is a CBOR encoded COSE_KeySet.";
        reference
          "I-D.amsuess-ace-brski-ace, Provisioning ACE credentials
          through BRSKI";
      }

      leaf ace-aud {
        type string;
        description
          "Audience identifier by which the ACE Authorization Server
          will be the pledge that is enrolled as an ACE Resource
          Server.";
        reference
          "I-D.amsuess-ace-brski-ace, Provisioning ACE credentials
          through BRSKI";
      }
    }
  }
}


<CODE ENDS>
```

A device accepting this voucher will accept tokens signed with the credials expressed as a COSE key in the ace-as-pubk field, provided they are issued with an audience value of "jada89".

3. Security Considerations

[TBD; in particular the open question on symmetric keys.]

4. IANA Considerations

[TBD: Request this for the YANG Module Names Registry; the module itself is registered differently.]

5. Open questions

* There are probably missing steps in this specification; the current draft's intention is primarily to start discussion.

* Is there a shorter route to the same result I missed (and should take instead)?

  Is there a longer route (doing EST style onboarding into a PKI, and then obtain AS data by using those certificates) that I missed (and could reference and learn from)?

* Is there existing YANG terminology for ACE (or just OAuth) to use?

  There was some OAuth in the YANG of draft-kwatsen-netconf-http-client-server-03, but that was just FIXMEs, and later removed.

* AIU the voucher artifact data assembled by the registrar travels to the MASA to be signed during BRSKI. That's fine when we're shipping a pinned-domain-cert, and also when we're shipping as-public-key and an audience identifier (for the ACE EDHOC profile), but not when shipping a shared key (for the ACE OSCORE profile).

* Is this suitable use of BRSKI and the voucher?

* This document currently only describes expressing the ACE details in YANG for an ACE voucher.

  For use with more EST-like enrollments, it could define resources equivalent to the rt=ace.est.sen resources.

  Alternatively, such setups could use COMI to manipulate the AS. (But in the EST direction, would this need "pull mode COMI"?)

6. References

6.1. Normative References

[CWT] Jones, M., Wahlstroem, E., Erdtman, S., and H. Tschofenig, "CBOR Web Token (CWT)", RFC 8392, DOI 10.17487/RFC8392, May 2018, <https://www.rfc-editor.org/rfc/rfc8392>.

[_8366bis] Watsen, K., Richardson, M., Pritikin, M., Eckert, T. T., and Q. Ma, "A Voucher Artifact for Bootstrapping Protocols", Work in Progress, Internet-Draft, draft-ietf-anima-rfc8366bis-07, 7 February 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-anima-rfc8366bis-07>.

6.2. Informative References

[ace-oscore] Palombini, F., Seitz, L., Selander, G., and M. Gunnarsson, "The Object Security for Constrained RESTful Environments (OSCORE) Profile of the Authentication and Authorization for Constrained Environments (ACE) Framework", Work in Progress, Internet-Draft, draft-ietf-ace-oscore-profile-19, 6 May 2021, <https://datatracker.ietf.org/doc/html/draft-ietf-ace-oscore-profile-19>.

[authz] Selander, G., Mattsson, J. P., Vučinić, M., Richardson, M., and A. Schellenbaum, "Lightweight Authorization for EDHOC", Work in Progress, Internet-Draft, draft-selander-lake-authz-02, 21 April 2023, <https://datatracker.ietf.org/doc/html/draft-selander-lake-authz-02>.

Acknowledgments

TODO acknowledge.

Author's Address

Christian Amsüss
Austria

Email: christian@amsuess.com