Network Working Group
Internet-Draft
Intended status: Informational
Expires: September 27, 2015

M. Richardson
SSW

March 26, 2015

X509.v3 certificate extension for authorization of device ownership draft-richardson-6tisch-idevid-cert-01

Abstract

This document details an X.509 extension to provide authorization and indication of ownership of a constrained device containing 802.1AR IDevID.

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 http://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 September 27, 2015.

Table of Contents

1. Introduction

This document defines two X.509 v3 certificate extensions that authorize the transfer of the right-to-use for a set of devices identified by 802.1AR IDevID from a production Factory through national and regional distributors (VARs) to Plant Owners/Operators. This extension binds a list of IDevID identifiers to the subject (private key holder) of a certificate. The issuer of the certificate is an entity (e.g., a Factory) that has produced the device to to transfer ownership set of IDevID to the subject of the certificate. These certificates provide a scalable, no-touch means of verifying the ownership of a constrainted device. The constrained is initialized with the trusted certificate of the Factory at the Factory. This process may be used by enrollment protocols such as 1x, PANA, EAP-TLS and RPL to validate that the network infrastructure being presented is the legitimate infrastructure for the constrainted device.

Sections 2 specify several rules about the encoding of the extensions defined in this specification that MUST be followed. These encoding rules serve the following purposes. First, they result in a unique encoding of the extension's value; two instances of an extension can be compared for equality octet-by-octet. Second, they achieve the minimal size encoding of the information. Third, they allow relying parties to use one-pass algorithms when performing certification path validation; in particular, the relying parties do not need to sort the information, or to implement extra code in the subset checking algorithms to handle several boundary cases (adjacent, overlapping, or subsumed ranges).

1.1. Terminology

It is assumed that the reader is familiar with the terms and concepts described in "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" [RFC3280], "INTERNET PROTOCOL" [RFC791], "Internet Protocol Version 6 (IPv6) Addressing Architecture" [RFC3513], "INTERNET REGISTRY IP ALLOCATION GUIDELINES" [RFC2050], and related regional Internet registry address management policy documents. Some relevant terms include:

allocate - the transfer of custodianship of a resource to an intermediate organization (see [RFC2050]).

assign - the transfer of custodianship of a resource to an end organization (see [RFC2050]).

Autonomous System (AS) - a set of routers under a single technical administration with a uniform policy, using one or more interior gateway protocols and metrics to determine how to route packets within the autonomous system, and using an exterior gateway protocol to determine how to route packets to other autonomous systems.

Autonomous System number - a 32-bit number that identifies an autonomous system.

delegate - transfer of custodianship (that is, the right-to-use) of an IP address block or AS identifier through issuance of a certificate to an entity.

initial octet - the first octet in the value of a DER encoded BIT STRING [X.690].

IDevID - a variable octet identifier written as in hexadecimal. While there is no length limit to the IDevID, a Factory is expected to pick a particularly length and stick to that length so that the IDevID can be aggregated by simple integer enumeration.

subsequent octets - the second through last octets in the value of a DER encoded BIT STRING [X.690].

trust anchor - a certificate that is to be trusted when performing certification path validation (see [RFC3280]).

The keywords MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD, SHOULD NOT, RECOMMENDED, and MAY, and OPTIONAL, when they appear in this document, are to be interpreted as described in [RFC2119].

2. Autonomous System Identifier Delegation Extension

This extension conveys the delegation of ownership of a device identified by an 802.1AR Device ID to an entity by binding those IDevID to a public key belonging to the entity.

2.1. Context

802.1AR defines a mechanism by which a manufacturer may place a certificate that attests to the a device's identity into the device at manufacturer time. This mechanism permits a device to cryptographically identify itself to a network. The device, however is unable to know to which network it belongs. This extension permits the manufacturer, using the same trusted anchor to delegate ownership of the device to the end user (possibly via a series of intermediaries, such as a supplier chain). The use of such a certificate chain can be easily verified by the device, and therefore, combined with 802.1AR, permits mutual authentication of devices and network entities.

2.2. Specification

The OID for this extension is id-pe-iDevID.

```
id-pe-iDevID OBJECT IDENTIFIER ::= { id-pe IANA-TBD }
where [RFC3280] defines:

id-pkix OBJECT IDENTIFIER ::= { iso(1) identified-organization(3)
    dod(6) internet(1) security(5) mechanisms(5) pkix(7) }

id-pe OBJECT IDENTIFIER ::= { id-pkix 1 }
```

Figure 1: OID

2.2.1. Criticality

This extension SHOULD be CRITICAL. The intended use of this extension is to connote an ownership of the device specified in the extension. A CA marks the extension as CRITICAL to convey the notion that a relying party must understand the semantics of the extension to make use of the certificate for the purpose it was issued. Newly created applications that use certificates containing this extension are expected to recognize the extension.

2.2.2. Syntax

```
id-pe-iDevID OBJECT IDENTIFIER ::= { id-pe IANA_TBD }

IDevID ::= SEQUENCE { idevnum [0] EXPLICIT
            IDevIDChoice OPTIONAL,
            rdi [1] EXPLICIT ASIdentifierChoice OPTIONAL
       }

IDevIDChoice ::= CHOICE { inherit NULL, -- inherit from issuer --
            iDevIdsOrRanges SEQUENCE OF iDevIdOrRange
       }

IDevIdOrRange ::= CHOICE { id IDevId, range IDevRange }
IDevRange ::= SEQUENCE { min IDevId, max IDevId }
IDevId ::= INTEGER
```

Figure 2: OID

2.2.3. Type IDevID

The IDevID type is a SEQUENCE containing one or more forms of Device Identifiers-- IDevID numbers (in the idevnum element) or routing domain identifiers (in the rdi element). When the IDevID type contains multiple forms of identifiers, the idevnum entry MUST precede the rdi entry. IDevID numbers are used by 802.1AR and are specified there.

2.2.4. Elements asnum, rdi, and Type ASIdentifierChoice

The idevnum and rdi elements are both of type IDevIDChoice. The IDevIDChoice type is a CHOICE of either the inherit or asIdsOrRanges element.

XXX - But I don't think we need this CHOICE

2.2.5. Element inherit

If the IDevIDChoice choice contains the inherit element, then the set of authorized IDevIDs is taken from the issuer's certificate, or from the issuer's issuer's certificate, recursively, until a certificate containing an IDevIDChoice containing an iDevIdsOrRanges element is located. If no authorization is being granted for a particular form of IDevID, then there MUST NOT be a corresponding idevnum/rdi member in the IDevID sequence.

2.2.6. Element asIdsOrRanges

The asIdsOrRanges element is a SEQUENCE of ASIdOrRange types. Any pair of items in the asIdsOrRanges SEQUENCE MUST NOT overlap. Any contiguous series of AS identifiers MUST be combined into a single range whenever possible. The AS identifiers in the asIdsOrRanges element MUST be sorted by increasing numeric value.

2.2.7. Type ASIdOrRange

The ASIdOrRange type is a CHOICE of either a single integer (IDevId) or a single sequence (IdevIDRange).

2.2.8. Element id

The id element has type ASId.

2.2.9. Element range

The range element has type ASRange.

2.2.10. Type IDevIDRange

The IDevIDRange type is a SEQUENCE consisting of a min and a max element, and is used to specify a range of IDevID identifier values.

2.2.11. Elements min and max

The min and max elements have type IDevID. The min element is used to specify the value of the minimum IDevID identifier in the range, and the max element specifies the value of the maximum IDevID identifier in the range.

2.2.12. Type IDevId

The IDevId type is an INTEGER. XXX - this will need work

2.3. Autonomous System Identifier Delegation Extension Certification

Path Validation

Certification path validation of a certificate containing the autonomous system identifier delegation extension requires additional processing. As each certificate in a path is validated, the AS identifiers in the autonomous system identifier delegation extension of that certificate MUST be subsumed by the AS identifiers in the autonomous system identifier delegation extension in the issuer's certificate. Validation MUST fail when this is not the case. A certificate that is a trust anchor for certification path validation of certificates containing the autonomous system identifier delegation extension, as well as all certificates along the path, MUST each contain the autonomous system identifier delegation extension. The initial set of allowed AS identifiers is taken from the trust anchor certificate.

3. Security Considerations

This specification describes an X.509 extension. Since X.509 certificates are digitally signed, no additional integrity service is necessary. Certificates with these extensions need not be kept secret, and unrestricted and anonymous access to these certificates has no security implications.

However, security factors outside the scope of this specification will affect the assurance provided to certificate users. This section highlights critical issues that should be considered by implementors, administrators, and users.

This extensions represent authorization information, i.e., a right-to-use/ownership statement for a device. They were developed to support zero-touch autonomic configuration of constrained devices in a sensor network. As a result of this capability model, the Subject field is largely irrelevant for security purposes, contrary to common PKI conventions.

4. Acknowledgments

This document was cribbed extensively from RFC3779, however, errors were introduced here.

5. Appendix A -- ASN.1 Module

This normative appendix will describes the IDevID extensions used by conforming PKI components in ASN.1 syntax.

6. Appendix C -- Example of an AS Identifier Delegation Extension

A critical X.509 v3 certificate extension that specifies:

7. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

Author's Address

Michael C. Richardson
Sandelman Software Works
470 Dawson Avenue
Ottawa, ON K1Z 5V7
CA

Email: mcr+ietf@sandelman.ca
URI: http://www.sandelman.ca/