Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: May 3, 2018

O. Friel
R. Barnes
Cisco

October 30, 2017

PKI Certificate Identifier Format for Devices
draft-friel-pki-for-devices-00

Abstract

This document defines a standard Subject field identifier format for certificates issued to Internet of Things (IoT) devices. This will allow applications to easily and uniquely identify certificates issued to devices as opposed to certificates issue to services or users. The certificates will adhere to standard Web PKI specifications thus ensuring interoperability with existing Certificate Authorities processes and workflows, and standard client and service libraries and applications.

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 May 3, 2018.

Table of Contents

1. Introduction

There is an increasing need for devices to be able to uniquely identify themselves and assert their identity, and associated identity attributes, using standard Web PKI techniques. In order to faclitate issuing certificates to devices, this document defines a mechanism for uniquely identifying devices using a structured Subject field identifier that should be supported by all major Certificate Authorities (CAs), including those CAs that support [I-D.ietf-acme-acme].

The use of Web PKI for the purpose of issuing device certificates has multiple benefits including:

- Existing code, processes, and policies for managing Web PKI certificates can be re-used
- Device certificates can be trusted by web browsers
- For small-scale device manufacturers, it is possible to use existing CAs to issue device certificates of this kind
- For more mature manufacturers, the use of structured DNS names to encode device information means that name-constrained intermediate CAs can be used to allow the manufacturer to issue device certificates independently of the root CA.

Previous attempts to uniquely identify device certificates have not proven to be broadly supported by common certificate management software libraries. These include:

- [IEEE802.1AR] which defines a serialNumber field
- [RFC4108] which defines a hardwareModuleName field

2. Manufacturing vs. Deploy Time Certificates

Devices will typically have a unique certificate that is baked into the device at manufacturing time i.e. the device will leave the factory with a unique manufacturer installed certificate already baked in. This certificate will typically be signed by a CA that the manufacturer controls, or a CA that the manufacturer explicitly authorizes. This CA does not necessarily have be a public root CA that is trusted by web browsers. This certificate is referred to as the Initial Device Identifier (IDevID).

A common deployment requirement is that the end customer that purchases and deploys the device in their local domain will need to install a certificate on the device that is signed by a CA under their control, or signed by a CA of their choosing. This certificate is referred to as the Locally Significant Device Identifier (LDevID).

3. Device Information Domain Name

A unique device identifier is encoded in a structured Device Information Domain Name Identifier (DIDN-ID) of the following form:

<serial>.<model>.keyword.<domain>

where "keyword" MUST be one of:

_mDevice
_device

The fields "serial", "model" and "domain" are described in the following sections.

3.1. IDevID Certificates

IDevID certificates have the following form:

<serial>.<model>._mDevice.<manufacturer>

Where:

- "manufacturer" is a fully-qualified domain name identifying the manufacturer of the device

- "_mDevice" is a mandatory keyword that indicates this is an IDevID installed at manufacturing time

- "model" is a manufacturer-chosen string that MUST identify the model or type of the device

- "serial" is a manufacturer-chosen string that MUST identify the specific serial number of this model

The combination of "manufacturer", "model", and "serial" MUST uniquely identify the device.

3.2. LDevID Certificates

If the LDevID is issued by a public trusted CA, then the LDevID idenfitier format MUST follow the identifier format specified in this section.

Where the LDevIDs are issued by private domain CAs that do not necessarily need to adhere to CA/Browser forum guidelines, it is strongly recommended that the private CA follows this identifier format specification.

LDevID certificates have the following form:

```
<serial>.<type>._device.<deployment-domain>
```

Where:

- "deployment-domain" is a fully-qualified domain name identifying the local domain where the device is installed. This will typically be a domain that the purchaser or owner of the device can assert ownership of

- "_device" is a mandatory keyword that indicates this is an LDevID installed during live deployment

- "model" this SHOULD be copied from the IDevID of the device

- "serial" this SHOULD be copied from the IDevID of the device

The combination of "manufacturer", "model", and "serial" SHOULD uniquely identify the device.

If the customer who owns the device uses a public CA to issue the LDevID, and if the device "serial" number and/or "model" is considered sensitive or Personally Identifiable Information (PII), then the "serial" and "model" fields MAY be replaced with suitable alternate identifiers. However, the public CA MUST ensure that the format and structure of the DIDN-ID adheres to this specification.

4. Certificate Fields

4.1. Subject

Following the recommendations set out in [RFC6125], the Subject field of the certificate MAY contain the "commonName" field, set to the DIDN-ID for the device.

The Subject field MAY also contain a "serialNumber" or "hardwareModuleName" field.

4.2. Subject Alternate Name

The certificate MUST contain a "subjectAltName" extension contataining a single "dnsName" entry with the DIDN-ID for the device.

4.3. Extended Key Usage

The certificate MUST contain an "extKeyUsage" extension with the values "id-kp-serverAuth" and "id-kp-clientAuth", and no other values.

4.4. Certificate Lifetime

IDevID certificates with "_mDevice" identifiers in their DIDN-ID MUST have a "notAfter" value of 99991231235959Z (i.e. Y10K).

It should be noted that at the time of writing, web browsers do not check for Y10K and will happily establish connections with endpoints whose identity certificate has a "notAfter" value of Y10K.

LDevID certificates are issued during live deployment and MUST follow the standard lifetime and expiration requirements of the issuing CA.

5. IANA Considerations

[[TODO: Register the "_device" and "_mDevice" labels]]

6. Security Considerations

[[TODO]]

7. Informative References

[I-D.ietf-acme-acme]
Barnes, R., Hoffman-Andrews, J., and J. Kasten, "Automatic Certificate Management Environment (ACME)", draft-ietf-acme-acme-07 (work in progress), June 2017.

[IEEE802.1AR]
IEEE, ., "Secure Device Identity", 2017.

[RFC4108] Housley, R., "Using Cryptographic Message Syntax (CMS) to Protect Firmware Packages", RFC 4108, DOI 10.17487/RFC4108, August 2005, <https://www.rfc-editor.org/info/rfc4108>.

[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/info/rfc6125>.

Authors' Addresses

Owen Friel
Cisco

Email: ofriel@cisco.com

Richard Barnes
Cisco

Email: rlb@ipv.sx