Abstract

This informational document details the mechanism used by the CIRA Secure Home Gateway (SHG) to load MUD definitions for devices which have no integrated MUD (RFC8520) support.

The document describes extensions to the WiFi Alliance DPP QR code to support the use of MUD URLs.

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 29 June 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text.
as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction ........................................... 2
2. Terminology ........................................... 3
3. Protocol ............................................... 3
4. Privacy Considerations ................................. 4
5. Security Considerations ................................ 4
6. IANA Considerations .................................... 5
7. Acknowledgements ....................................... 5
8. References ............................................... 5
   8.1. Normative References ................................. 5
   8.2. Informative References ............................... 6
Authors’ Addresses ......................................... 7

1. Introduction

The Manufacturer Usage Description (MUD) [RFC8520] defines a YANG data model to express what sort of access a device requires to operate correctly. The document additionally defines three ways for the device to communicate the URL of the resulting JSON [RFC8259] format file to a network enforcement point: DHCP, within an X.509 certificate extension, and via LLDP.

Each of the above mechanism conveys the MUD URL inband, and requires modifications to the device firmware. Most small IoT devices do not have LLDP, and have very restricted DHCP clients. Adding the LLDP or DHCP options requires at least some minimal configuration change, and possibly entire new subsystems. The X.509 certificate extension only makes sense to deploy as part of a larger IDevID based [ieee802-1AR] system such as [I-D.ietf-anima-bootstrapping-keyinfra].

In all cases these mechanisms can only be implemented by persons with access to modify and update the firmware of the device. The MUD system was designed to be implemented by Manufacturers after all!

In the meantime there is a chicken or egg problem ([chickenegg]): no manufacturers include MUD URLs in their products as there are no gateways that use them. No gateways include code that processes MUD URLs as no products produce them.

The mechanism described here allows any person with physical access to the device to affix a reference to a MUD URL that can later be scanned by an end user. This can be done by the (marketing department) of the Manufacturer, by an outsourced assembler plant, by value added resellers, by a company importing the product (possibly
to comply with a local regulation), by a network administrator
(perhaps before sending devices home with employees), or even by a
retailer as a value added service.

The mechanism uses the QRcode, which is informally described in
[qrcode]. QR code generators are available as web services
([qrcodewebservice]), or as programs such as [qrencode]. They are
formally defined in [isoiec18004].

This document details how the CIRALabs Secure Home Gateway encode MUD
URLs as QR codes.

A issue addressed by this document is the question of whether and
when the MUD file should be specific to a specific version of the
device firmware.

The third issue is that an intermediary (ISP, or third-party security
service) may want to extend or amend a MUD file received from a
manufacturer. In order to maintain an audit trail of changes, a way
to encode the previous MUD URL and signature file (and status) is
provided. (FOR DISCUSSION)

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
"SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and
"OPTIONAL" in this document are to be interpreted as described in
BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all
capitals, as shown here.

3. Protocol

The [dpp] specification from the Wi-Fi Alliance has created a base
for a QRcode based enrollment system. This specification extends it
to include a MUD URL.

The QR code is as specified in section 5.2.1 of [dpp] is repeated
here:

    dpp-qr = âDPP:â [channel-list â;â] [mac â;â]
    [information â;â] public-key â;;â

This is amended as follows:

    dpp-qr = âDPP:â [channel-list â;â] [channel-list â;â]
    [mac â;â] [information â;â] public-key
    [";" mudurl ] â;;â

mudurl = "D:" *(%x20-3A / %x3C-7E) ; semicolon not allowed
While the ABNF defined in the [dpp] document assumes a specific order (C:, M:, I:, K:), this specification relaxes this so that the tags can come in any order. However, in order to make interoperation with future DPP-only clients as seamless as possible, the MUD extension suggested here are placed after those defined in [dpp].

This document establishes an IANA registry for DPP attributes.

The syntax of the QR code definition given above does not permit a semicolon to be included. Semicolons (";") would otherwise be permitted in MUD URLs. This restriction on the content the URL is not considered a concern as it is uncommon to use them in a URL.

The URL provided MUST NOT have a query (?) portion present.

An IANA registry is created for the attributes below.

4. Privacy Considerations

TBD.

5. Security Considerations

The security of the Device Provisioning Protocol is enhanced when the public key for a device is not available without physical access to the device. Placement of a QR code for use by a MUD controller has no such dependancy, and so such QR codes may be affixed in prominant places on the outside of packaging. This is not a recommended practice as future versions of the sticker may include full DPP information.

The QRcode described in this document is identical for all instances of the device, and the stickers may be mass produced. The situation is not the same when a full DPP content is present: each sticker is unique. A manufacturing plant designed to affix MUD URLs may get confused and not be ready for the full DPP.

It is recommended that the manufacturing process be designed with the full DPP process -- unique QR codes per device -- initially so that no changes are necessary when/if DPP is introduced.
6. IANA Considerations

IANA is requested to create a new Registry entitled: "Device Provisioning Protocol Attributes". New items can be added to using Specification Required. In order to conserve space, registrations are expected to be single upper-case ASCII letters, but the Expert Reviewer MAY make exceptions. No entry may contain a colon. All entries beginning with "X" are reserved as Private-Use values.

The following items are to be added to the initial table:

+--------+--------------+-----------------+
| Letter |     Name     | Document        |
|--------+--------------+-----------------|
| C      | channel-list | [dpp]           |
| M      | MAC address  | [dpp]           |
| I      | information  | [dpp]           |
| K      | public key   | [dpp]           |
| D      | MUD URL      | [This document] |
+--------+--------------+-----------------+

Table 1

(Editorial Note: the authors of the DPP specification have consented to seeding control to IANA)

7. Acknowledgements

This work was supported by the Canadian Internet Registration Authority (cira.ca).

8. References

8.1. Normative References


8.2. Informative References


Authors’ Addresses

Michael Richardson
Sandelman Software Works
Email: mcr+ietf@sandelman.ca

Jacques Latour
CIRA Labs
Email: Jacques.Latour@cira.ca