GLOBALPLATFORM®
THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

GlobalPlatform Technology
MUD Device Testing Plan
Version 0.0.0.3

Public Review

June 2021

Document Reference: GPI_TEN_001

Copyright © 2020-2021 GlobalPlatform, Inc. All Rights Reserved.
Recipients of this document are invited to submit, with their comments, notification of any relevant patents or other intellectual property rights (collectively, "IPR") of which they may be aware which might be necessarily infringed by the implementation of the specification or other work product set forth in this document, and to provide supporting documentation. This document is currently in draft form, and the technology provided or described herein may be subject to updates, revisions, extensions, review, and enhancement by GlobalPlatform or its Committees or Working Groups. Prior to publication of this document by GlobalPlatform, neither Members nor third parties have any right to use this document for anything other than review and study purposes. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

THIS SPECIFICATION OR OTHER WORK PRODUCT IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NON-INFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY IMPLEMENTATION OF THIS SPECIFICATION OR OTHER WORK PRODUCT SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER THE COMPANY, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY IMPLEMENTER OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER DIRECTLY OR INDIRECTLY ARISING FROM THE IMPLEMENTATION OF THIS SPECIFICATION OR OTHER WORK PRODUCT.

This document is provided as a member benefit to GlobalPlatform members only.
Please help us maintain the value of your membership and encourage recruitment by observing this restriction.

Copyright © 2020-2021 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Contents

Tables

Copyright © 2020-2021 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

1 Introduction

This plan addresses three topics: device support for Manufacturer Usage Descriptions, availability and correctness of a MUD file, and proper coverage of access by a device. The basis of this work is [RFC 8520].

1.1 Audience

This document is intended primarily for the use of device manufacturers and laboratories that want to test the implementation of a device supporting a MUD file.

1.2 IPR Disclaimer

Attention is drawn to the possibility that some of the elements of this GlobalPlatform specification or other work product may be the subject of intellectual property rights (IPR) held by GlobalPlatform members or others. For additional information regarding any such IPR that have been brought to the attention of GlobalPlatform, please visit https://globalplatform.org/specifications/ip-disclaimers/. GlobalPlatform shall not be held responsible for identifying any or all such IPR, and takes no position concerning the possible existence or the evidence, validity, or scope of any such IPR.

1.3 References

The tables below list references applicable to this specification. The latest version of each reference applies unless a publication date or version is explicitly stated.

Table 1-1: Normative References

Standard / Specification	Description	Ref
IETF RFC 8520	Specification of a component-based architecture for Manufacturer Usage Descriptions (MUDs)	[RFC 8520]
IETF RFC 7159	Specification of JavaScript Object Notation (JSON) – a lightweight, text-based, language-independent data interchange format	[RFC 7159]
IETF RFC 3986	Uniform Resource Identifier (URI): Generic Syntax	[RFC 3986]
IETF RFC 3987	Internationalized Resource Identifiers (IRIs)	[RFC 3987]
IETF RFC 2119	Key words for use in RFCs to Indicate Requirement Levels	[RFC 2119]

Table 1-2: Informative References

Standard / Specification	Description	Ref
IEEE 802.1AB	Station and Media Access Control Connectivity Discovery	
IETF RFC 1531	Dynamic Host Configuration Protocol	

Copyright © 2020-2021 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

1.4 Terminology and Definitions

The following meanings apply to SHALL, SHALL NOT, MUST, MUST NOT, SHOULD, SHOULD NOT, and MAY in this document (refer to [RFC 2119]):

- **SHALL** indicates an absolute requirement, as does **MUST**.
- **SHALL NOT** indicates an absolute prohibition, as does **MUST NOT**.
- **SHOULD** and **SHOULD NOT** indicate recommendations.
- **MAY** indicates an option.

1.5 Abbreviations and Notations

Table 1-3: Abbreviations and Notations

Abbreviation / Notation	Meaning
DHCP	Dynamic Host Configuration Protocol
LLDP	Link Layer Discovery Protocol
MUD	Manufacturer Usage Description
TLV	Tag Length Value

1.6 Revision History

GlobalPlatform technical documents numbered *n*.0 are major releases. Those numbered *n*.1, *n*.2, etc., are minor releases where changes typically introduce supplementary items that do not impact backward compatibility or interoperability of the specifications. Those numbered *n.n*.1, *n.n*.2, etc., are maintenance releases that incorporate errata and precisions; all non-trivial changes are indicated, often with revision marks.

Table 1-4: Revision History

Date	Version	Description
Dec 2020	0.0.0.1	Task Force Review
April 2021	0.0.0.3	Member Review
TBD	1.0	Initial release

Copyright © 2020-2021 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

2 Main Requirements

2.1 Device Support for a MUD File

Device support may be provided in one of three ways to indicate the MUD URL: use of LLDP, DHCP, or an X.509 certificate via EAP-TLS or TEAP. Thus a device must meet only one of the following three requirements:

R1.1 Proper Emission via DHCP

Device emits a well-formed DHCP packet that contains a TLV that is formatted as described in [RFC 8520] section 10. A MUD URL is like any other URL, and must validate as such, as specified in [RFC 3986] and [RFC 3987]. This may be observed with Wireshark or TCPDUMP. A MUD URL validator can be found at https://github.com/CiscoDevNet/MUD-URL-Validator/blob/master/validate_mud_url.py.

R1.2 Proper Emission via X.509 Certificate

Device emits a well-formed certificate that contains the extensions that are specified in [RFC 8520] section 11. This may be tested by receiving the certificate with EAP-TLS and a Radius server.

R1.3 Proper Emission via LLDP

Device emits a well-formed LLDP packet that contains a TLV that is formatted as described in [RFC 8520] section 12. This may be observed with Wireshark or TCPDUMP. A MUD URL validator can be found at https://github.com/CiscoDevNet/MUD-URL-Validator/blob/master/validate_mud_url.py.

2.2 Availability and Correctness of the MUD File

R2.1 MUD File Availability

The MUD file must be available on an HTTP public service that the MUD URL points to. This can be tested with the wget tool and retrieved using $MUDURL.

R2.2 Valid JSON

The file returned must be valid JSON as defined in [RFC 7159]. This can be tested with JSON validators, such as that found at jsonformatter.curiousconcept.com.

Copyright © 2020-2021 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

R2.3 Valid Serialized MUD

The MUD file itself must contain all mandatory attributes specified in [RFC 8520]. Specifically this includes: `mud-version`, which must be set to 1.1; `mud-url`; `last-update`; and `is-supported`. NO OTHER ATTRIBUTES ARE REQUIRED IN THE MUD FILE. However, those present must comport with their form and substance as specified in [RFC 8520].

R2.4 Valid Signature

If `mud-signature` is present in the MUD file, the signature must be resolvable via HTTP and must validate against a provided trust anchor. A signature can be validated with the following OpenSSL command:

```
% openssl cms -in mudfile.p7s -binary -content mudfile.json -CAfile root.crt -out
/dev/null
```

2.3 Access Control Statements

This section is applicable if the MUD file contains access-list statements.

R3.1 Use of to-device-policy and from-device-policy

If access control statements are present, they must conform in form and substance to [RFC 8520]. Specifically, IPv4 and/or IPv6 ACLs must be named in respective `to-device-policy` and `from-device-policy` arrays.

This can be validated via either the MUD file pretty printer parser or the MUD file visualizer on mudmaker.org.

R3.2 ACLs Properly Describe Device Behavior

ACLs must cover all **LAYER 3** packets to and from device that the device is expected to emit, except DNS and NTP packets. At the time of this writing, MUD doesn't specify L2 ACL support. DHCP packets, for example, between the device and a switch, or any 802.11 frames that are not IP are beyond the scope of MUD and this test specification.

To test this, the MUD file should be examined to determine which abstractions are being used. For each abstraction, a table must be created to indicate how it is expected to be populated. After that, the device should be exercised for all conditions it would operate in. This includes exceptional conditions, such as various fault modes it might encounter. A PCAP file should be collected.

Once the PCAP file is collected, the L3 packets to and from the device should be examined to determine if they match any entry in the table that was created. If not, the test has failed.

Copyright © 2020-2021 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.