

pkix
Internet-Draft
Intended status: Standards Track
Expires: August 5, 2016

E. Lear
Cisco Systems
February 02, 2016

**An X.509 Extension for Manufacturer Usage Description URI
draft-lear-ietf-pkix-mud-extension-00**

Abstract

Manufacturer User Descriptions are used by device manufacturers to provide indications to the network as to the intended use of a particular device and with what end points it might communicate. A URI points to those descriptions. This memo specifies an X.509 certificate extension to specify that URI in a device certificate to be used with IEEE 802.1AR.

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 August 5, 2016.

Copyright Notice

Copyright (c) 2016 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 (<http://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.](#) The Manufacturer Usage Description (MUD) URI Extension . . . [2](#)
- [3.](#) Security Considerations [3](#)
- [4.](#) IANA Considerations [3](#)
- [5.](#) Acknowledgments [3](#)
- [6.](#) References [3](#)
 - [6.1.](#) Normative References [3](#)
 - [6.2.](#) Informative References [4](#)
- Author's Address [4](#)

1. Introduction

[I-D.lear-mud-framework] introduces the concept of manufacturer usage description. In other documents, DHCP is used to identify a URI that network systems can use to retrieve YANG-based XML that advises the network on appropriate usage of a device.

Use of DHCP as a means of transmission may not be appropriate for all use cases, particularly for devices intended for use in critical environments. The IEEE has developed [[IEEE8021AR](#)] that provides a certificate-based approach to communicate device characteristics, which itself relies on [[RFC5280](#)].

This document specifies an X.509 extension so that such MUD URI may be communicated via 802.1AR. The MUD URI extension is non-critical, as required by IEEE 802.1AR.

2. The Manufacturer Usage Description (MUD) URI Extension

[RFC7299] provides a procedure and means to specify extensions to X.509 certificates. The object identifier (OID) for extensions is as follows:

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

The choice of id-pe is based on guidance found in [Section 4.2.2 of \[\[RFC5280\]\(#\)\]](#):

These extensions may be used to direct applications to on-line information about the issuer or the subject.

Lear

Expires August 5, 2016

[Page 2]

The MUD URI is precisely that: online information about the particular subject.

The new extension is identified as follows:

- The MUD URI extension id-pe-mud-uri OBJECT IDENTIFIER ::= { id-pe TBD }

The extension returns a single value:

mud-uri ::= uniformResourceIdentifier - for use with mud architecture.

The semantics of the URI are defined [[I-D.lear-ietf-netmod-mud](#)].

3. Security Considerations

This document specifies a certificate extension to communicate a Manufacturer Usage Description URI. The semantics of the URI are defined in [draft-lear-ietf-netmod-mud](#). At this time, no security concerns are visible to the author for inclusion of such an extension.

4. IANA Considerations

The IANA is requested to assign a value for id-pe-mud-uri in the "SMI Security for PKIX Certificate Extension" Registry.

5. Acknowledgments

The author wishes to thank Max Pritikin for his review and suggestions.

6. References

6.1. Normative References

[I-D.lear-ietf-netmod-mud]

Lear, E., "Manufacturer Usage Description YANG Model", [draft-lear-ietf-netmod-mud-00](#) (work in progress), January 2016.

[RFC7299] Housley, R., "Object Identifier Registry for the PKIX Working Group", [RFC 7299](#), DOI 10.17487/RFC7299, July 2014, <<http://www.rfc-editor.org/info/rfc7299>>.

6.2. Informative References

[I-D.lear-mud-framework]

Lear, E., "Manufacturer Usage Description Framework",
[draft-lear-mud-framework-00](#) (work in progress), January
2016.

[IEEE8021AR]

Institute for Electrical and Electronics Engineers,
"Secure Device Identity", 1998.

[IEEE8021X]

Institute for Electrical and Electronics Engineers, "Port
Based Network Access Control", 1998.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S.,
Housley, R., and W. Polk, "Internet X.509 Public Key
Infrastructure Certificate and Certificate Revocation List
(CRL) Profile", [RFC 5280](#), DOI 10.17487/RFC5280, May 2008,
<<http://www.rfc-editor.org/info/rfc5280>>.

Author's Address

Eliot Lear
Cisco Systems
Richtistrasse 7
Wallisellen CH-8304
Switzerland

Phone: +41 44 878 9200
Email: lear@cisco.com

