

Device Owner Attribute
draft-turner-deviceowner-attribute-03.txt

Abstract

This document defines the Device Owner attribute. It indicates the entity (e.g., company, organization, department, agency) that owns the device. This attribute may be included in public key certificates and attribute certificates.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>

This Internet-Draft will expire on August 1, 2010.

Copyright Notice

Copyright (c) 2010 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.

1. Introduction

This document specifies the Device Owner attribute. It indicates the entity (e.g., company, organization, department, agency) that owns the device. This attribute is intended to be used in public key certificates [[RFC5280](#)] and attribute certificates [[RFC5755](#)].

This attribute may be used in automated authorization decisions. For example, when two peers are deciding whether to communicate each could check that the device owner present in the other device's certificate is on an "approved" list. This check is performed in addition to certification path validation [[RFC5280](#)]. The mechanism for managing the "approved" list is beyond the scope of this document.

NOTE: This document does not provide an equivalent LDAP schema specification as this attribute is targeted at public key certificates [[RFC5280](#)] and attribute certificates [[RFC5755](#)]. Definition of an equivalent LDAP schema is left to a future specification.

1.1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [[RFC2119](#)].

1.2. ASN.1 Syntax Notation

The attribute is defined using ASN.1 [[X.680](#)] through [[X.683](#)].

2. Device Owner

The Device Owner attribute indicates the entity (e.g., company, organization, department, agency) that owns the Device with which this attribute is associated. Device Owner is an object identifier.

The following object identifier identifies the Device Owner attribute:

```
id-deviceOwner OBJECT IDENTIFIER ::= {  
    joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101)  
    dod(2) infosec(1) attributes(5) 69  
}
```

The ASN.1 syntax for the Device Owner attribute is as follows:

```
at-deviceOwner ATTRIBUTE ::= {  
    TYPE                OBJECT IDENTIFIER  
    EQUALITY MATCHING RULE  objectIdentifierMatch  
    IDENTIFIED BY          id-deviceOwner  
}
```

There MUST only be one value of Device Owner associated with a device. Distinct owners MUST be represented in separate certificates.

3. Security Considerations

If this attribute is used as part of an authorization process, the procedures employed by the entity that assigns each value must ensure that the correct value is applied. Including this attribute in a public key certificate or attribute certificate ensures the value for the device owner is integrity protected.

4. IANA Considerations

None: All identifiers are already registered. Please remove this section prior to publication as an RFC.

5. References

5.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC5280] Cooper, D., et. al., "Internet X.509 Public Key Infrastructure Certificate and Certification Revocation List (CRL) Profile", [RFC 5280](#), May 2008.

[RFC5755] Farrell, S., Housley, R., and S. Turner, "An Internet Attribute Certificate Profile for Authorization", [RFC 5755](#), January 2010.

[RFCTBD] Schaad, J., and P. Hoffman, "New ASN.1 Modules for PKIX", [draft-ietf-pkix-new-asn1-07.txt](#), work-in-progress.

/**

RFC Editor: Please replace "RFCTBD" with "RFC####" where #### is the number of the published RFC. Please do this in both the references and the text.

**/

[X.501] ITU-T Recommendation X.520 (2002) | ISO/IEC 9594-2:2002, Information technology - The Directory: Models.

[X.680] ITU-T Recommendation X.680 (2002) | ISO/IEC 8824-1:2002, Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation.

[X.681] ITU-T Recommendation X.681 (2002) | ISO/IEC 8824-2:2002. Information Technology - Abstract Syntax Notation One: Information Object Specification.

[X.682] ITU-T Recommendation X.682 (2002) | ISO/IEC 8824-3:2002. Information Technology - Abstract Syntax Notation One: Constraint Specification.

[X.683] ITU-T Recommendation X.683 (2002) | ISO/IEC 8824-4:2002. Information Technology - Abstract Syntax Notation One: Parameterization of ASN.1 Specifications.

[5.2. Informative References](#)

None

[Appendix A](#). ASN.1 Module

This appendix provides the normative ASN.1 [\[X.680\]](#) definitions for the structures described in this specification using ASN.1 as defined in [\[X.680\]](#) through [\[X.683\]](#).

DeviceOwnerAttribute-2008

```
{ joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101)
  dod(2) infosec(1) module(0) id-deviceOwnerAttribute-2008(34) }
```

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

-- EXPORTS ALL --

IMPORTS

-- IMPORTS from New PKIX ASN.1 [\[RFC2804\]](#)

ATTRIBUTE

FROM PKIX-CommonTypes-2009

```
{ iso(1) identified-organization(3) dod(6) internet(1)
  security(5) mechanisms(5) pkix(7) id-mod(0)
  id-mod-pkixCommon-02(57) }
```

-- Imports from ITU-T X.501 [\[X.501\]](#)

objectIdentifierMatch

FROM InformationFramework

```
{ joint-iso-itu-t ds(5) module(1) informationFramework(1) 4 }
```

;

-- device owner attribute OID and syntax

```
id-deviceOwner OBJECT IDENTIFIER ::= {
  joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101)
  dod(2) infosec(1) attributes(5) 69
}
```

at-deviceOwner ATTRIBUTE ::= {

```
  TYPE                OBJECT IDENTIFIER
  EQUALITY MATCHING RULE  objectIdentifierMatch
  IDENTIFIED BY          id-deviceOwner
}
```

END

Author's Address

Sean Turner
IECA, Inc.
3057 Nutley Street, Suite 106
Fairfax, VA 22031
USA

EMail: turners@ieca.com