

Network Working Group  
Internet Draft  
Intended Status: Informational Track  
Expires: August 1, 2010

Sean Turner, IECA  
February 1, 2010

Clearance Sponsor Attribute  
draft-turner-clearancesponsor-attribute-03.txt

## Abstract

This document defines the clearance sponsor attribute. It indicates the entity that sponsored (i.e., granted) the clearance. This attribute is intended for use in public key certificates and attribute certificates that also include the clearance attribute.

## 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/lid-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

Internet-Draft

Clearance Sponsor Attribute

February 2010

(<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 clearance sponsor attribute. It is included in public key certificates [[RFC5280](#)] and attribute certificates [[RFC5755](#)]. This attribute is only meaningful as a companion of the clearance attribute [[RFC5755](#)]. The clearance sponsor is the entity (e.g., agency, department, or organization) that granted the clearance to the subject named in the certificate. For example, the clearance sponsor for a subject asserting the Amoco clearance values [[RFC3114](#)] could be "Engineering".

This attribute may be used in automated authorization decisions. For example, a web server deciding whether to allow a user access could check that the clearance sponsor present in the user'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 initially 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. Clearance Sponsor

The clearance sponsor attribute, which is only meaningful if the clearance attribute [[RFC5755](#)] is also present, indicates the sponsor

of the clearance of the subject with which this attribute is associated. The clearance sponsor attribute is a DirectoryString [[RFC5280](#)], which MUST use the UTF8String CHOICE, string with a minimum size of 1 characters and a maximum of 64 characters.

The following object identifier identifies the sponsor attribute:

```
id-clearanceSponsor OBJECT IDENTIFIER ::= {
    joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101)
    dod(2) infosec(1) attributes(5) 68
}
```

The ASN.1 syntax for the clearance sponsor attribute is as follows:

```
at-clearanceSponsor ATTRIBUTE ::= {
    TYPE                      DirectoryString { ub-clearance-sponsor }
                              ( WITH COMPONENTS { utf8String PRESENT } )
    EQUALITY MATCHING RULE   caseIgnoreMatch
    IDENTIFIED BY            id-clearanceSponsor
}

ub-clearance-sponsor INTEGER ::= 64
```

There MUST only be one value of clearanceSponsor associated with a particular certificate. Distinct sponsors MUST be represented in separate certificates.

When an environment uses the Clearance Sponsor attribute, it is important that the same representation of the sponsor be used throughout the environment (e.g., using the same acronym). Further, the value in this attribute is not meant to be globally unique. When included in certificates, it is unique within the scope of the issuer.

### [3.](#) Security Considerations

If this attribute is used as part of an authorization process, the procedures employed by the entity that assigns each clearance sponsor 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 clearance sponsor is integrity protected.

The certificate issuer and clearance sponsor are not necessarily the same entity. If they are separate entities, then the mechanism used by the clearance sponsor to convey to the certificate issuer that

clearance sponsor did in fact grant the clearance to the subject needs to be protected from unauthorized modification.

If two entities are verifying each other's certificates, they do not share the same issuer, and they use the same clearance sponsor value (e.g., a United Kingdom PKI includes "MoD" and a New Zealand PKI also includes "MoD"), then the relying party has two choices 1) accept the two as strings as equivalent 2) indicate the sponsor as well as the trust anchor. To solve this problem, a mechanism, which is out side the scope of this specification, could be developed to allow a relying party to group together issuers that share a same context within which sponsor names have a unique significance.

While values of DirectoryString can include the NUL (U+0000) code point, values used to represent clearance sponsors typically would not. Implementations of the caseIgnoreMatch rule must, per X.501, consider all of the assertion value and attribute value in matching and hence protect against truncation attacks.

#### [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

Turner

Expires April 1, 2010

[Page 4]

---

Internet-Draft

Clearance Sponsor Attribute

February 2010

and the text.

\*\*/

[X.520] ITU-T Recommendation X.520 (2002) | ISO/IEC 9594-6:2002, Information technology - The Directory: Selected Attribute Types.

[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

[RFC3114] Nicolls, W., "Implementing Company Classification Policy with the S/MIME Security Label", [RFC 3114](#), May 2002.

## [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 [\[X.683\]](#).

ClearanceSponsorAttribute-2008

```
{ joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101)
  dod(2) infosec(1) modules(0)
  id-clearanceSponsorAttribute-2008(35) }
```

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

-- EXPORTS ALL --

IMPORTS

-- Imports from New PKIX ASN.1 [\[RFCTBD\]](#)

DirectoryString

PKIX1Explicit-2009

```
{ iso(1) identified-organization(3) dod(6) internet(1)
  security(5) mechanisms(5) pkix(7) id-mod(0)
  id-pkix1-explicit-02(51) }
```

-- Imports from New PKIX ASN.1 [[RFCTBD](#)]

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.520 [[X.520](#)]

caseIgnoreMatch

FROM SelectedAttributeTypes

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

;

Turner

Expires April 1, 2010

[Page 6]

---

Internet-Draft

Clearance Sponsor Attribute

February 2010

-- sponsor attribute OID and syntax

id-clearanceSponsor OBJECT IDENTIFIER ::= {  
joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101)  
dod(2) infosec(1) attributes(5) 68  
}

at-clearanceSponsor ATTRIBUTE ::= {  
TYPE DirectoryString { ub-clearance-sponsor }  
( WITH COMPONENTS { utf8String PRESENT} )  
EQUALITY MATCHING RULE caseIgnoreMatch  
IDENTIFIED BY id-clearanceSponsor  
}

ub-clearance-sponsor INTEGER ::= 64

END

Author's Address

Sean Turner  
IECA, Inc.  
3057 Nutley Street, Suite 106

Fairfax, VA 22031  
USA

E-Mail: [turners@ieca.com](mailto:turners@ieca.com)

Turner

Expires April 1, 2010

[Page 7]