

IETF PKIX WG  
Internet Draft  
Intended Status: Standards Track  
Updates: [3281](#) (once approved)  
Expires: April 26, 2009

Stephen Farrell, Trinity College Dublin  
Russ Housley, Vigil Security  
Sean Turner, IECA  
October 26, 2008

An Internet Attribute Certificate Profile for Authorization: Update  
draft-ietf-pkix-3281update-01.txt

## Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of 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 April 26, 2008.

## Copyright Notice

Copyright (C) The IETF Trust (2008).

## Abstract

This document updates [RFC 3281](#). It incorporates verified errata.

---

Internet-Draft    Update: An Internet Attribute Certificate    Oct 2008

## Discussion

This draft is being discussed on the 'ietf-pkix' mailing list. To subscribe, send a message to [ietf-pkix-request@imc.org](mailto:ietf-pkix-request@imc.org) with the single word subscribe in the body of the message. There is a Web site for the mailing list at <http://www.imc.org/ietf-pkix/>.

## 1. Introduction

This document updates [[RFC3281](#)]. It incorporates verified errata. OLD text is replaced by NEW text.

### 1.1. Requirements 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](#)].

## 2. Changes to [Section 4.1](#)

Replace the following ASN.1 excerpt in [section 4.1](#). This change incorporates verified technical errata #303.

NOTE: The "," is moved on the version line.

OLD:

```
AttributeCertificateInfo ::= SEQUENCE {
    version                AttCertVersion  -- version is v2,
    holder                 Holder,
    issuer                 AttCertIssuer,
    signature              AlgorithmIdentifier,
    serialNumber           CertificateSerialNumber,
    attrCertValidityPeriod AttCertValidityPeriod,
    attributes             SEQUENCE OF Attribute,
    issuerUniqueID         UniqueIdentifier OPTIONAL,
    extensions             Extensions OPTIONAL
}
```

NEW:

```
AttributeCertificateInfo ::= SEQUENCE {  
    version             AttCertVersion,  -- version is v2  
    holder              Holder,  
    issuer              AttCertIssuer,  
    signature           AlgorithmIdentifier,  
    serialNumber        CertificateSerialNumber,  
    attrCertValidityPeriod AttCertValidityPeriod,  
    attributes          SEQUENCE OF Attribute,  
    issuerUniqueID      UniqueIdentifier OPTIONAL,  
    extensions          Extensions OPTIONAL  
}
```

### 3. Changes to [Section 4.3.2](#)

Replace the OLD text with the NEW text in [section 4.3.2](#). This incorporates verified technical errata #710.

NOTE: "Confirming" is replaced "Conforming".

OLD:

Note: [X.509-2000] defines the extension syntax as a "SEQUENCE OF Targets". Conforming AC issuer implementations MUST only produce one "Targets" element. Conforming AC users MUST be able to accept a "SEQUENCE OF Targets". If more than one Targets element is found in an AC, the extension MUST be treated as if all Target elements had been found within one Targets element.

NEW:

Note: [X.509-2000] defines the extension syntax as a "SEQUENCE OF Targets". Conforming AC issuer implementations MUST only produce one "Targets" element. Conforming AC users MUST be able to accept a "SEQUENCE OF Targets". If more than one Targets element is found in an AC, the extension MUST be treated as if all Target elements had been found within one Targets element.

#### 4. Changes to [Section 4.4.6](#)

Replace OLD1 text with NEW1 text. This change incorporates verified technical errata #302. Replace OLD2 text with NEW2 text. This change incorporates reported technical errata #1479.

NOTE for OLD1: The differences in tagging arose due to an unnoticed technical corrigendum (TC-2) being applied to the X.501 [[X.501-1997](#)]

Turner, et al.

Expires April 26, 2009

[Page 3]

---

Internet-Draft      Update: An Internet Attribute Certificate      Oct 2008

document during preparation of [[RFC3281](#)]. The X.501 format is the correct form. Implementers SHOULD modify their decoding functions to accept either format and, even if claiming [RFC 3281](#) conformance, SHOULD output the (correct) X.501 format.

NOTE for OLD2: The two changes 1) removing the IMPLICIT from the type line and 2) adding the EXPLICIT to the value line. Both changes are for clarity, for alignment with X.501, and do not change the bits on the wire. With respect to 1) the module uses IMPLICIT tags therefore the IMPLICIT in the type line is extraneous and is removed  
2) [1] ANY, [1] EXPLICIT ANY, and [1] IMPLICIT ANY all result in the same encoding therefore for alignment purposes with X.501:1997 the EXPLICIT is added.

OLD1:

```
Clearance ::= SEQUENCE {
    policyId          [0] OBJECT IDENTIFIER,
    classList         [1] ClassList DEFAULT {unclassified},
    securityCategories [2] SET OF SecurityCategory OPTIONAL
}
```

NEW1:

```
Clearance ::= SEQUENCE {
    policyId          OBJECT IDENTIFIER,
    classList         ClassList DEFAULT {unclassified},
    securityCategories SET OF SecurityCategory OPTIONAL
}
```

OLD2:

```
SecurityCategory ::= SEQUENCE {
```

```
    type    [0] IMPLICIT OBJECT IDENTIFIER,
    value    [1] ANY DEFINED BY type
}
```

NEW2:

```
SecurityCategory ::= SEQUENCE {
    type    [0] OBJECT IDENTIFIER,
    value    [1] EXPLICIT ANY DEFINED BY type
}
```

## [5. Changes to \[Section 7.1\]\(#\)](#)

Replace the OLD text with the NEW text. This change incorporates reported technical errata #304.

OLD:

The AC then contains the ciphertext inside its signed data. The EnvelopedData (id-envelopedData) ContentType is used, and the content field will contain the EnvelopedData type.

NEW:

Within EnvelopedData, the encapsulatedContentInfo identifies the content type carried withing the ciphertext. In this case, the contentType field of encapsulatedContentInfo MUST contain id-ct-attrCertEncAttrs, which has the following value:

```
attrCertEncAttrs OBJECT IDENTIFIER ::= {
    iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9)
    id-smime(16) id-ct(1) 14 }
```

## [6. Changes to \[Section 10\]\(#\)](#)

Replace the reference to X.501:1993 to X.501:1997. This change incorporates reported technical errata #1479.

NOTE: Clearance was defined in X.501:1993 not X.501:1997.

OLD:

[X.501-1993] ITU-T Recommendation X.501 : Information Technology - Open Systems Interconnection - The Directory: Models, 1993.

NEW:

[X.501-1997] ITU-T Recommendation X.501 : Information Technology - Open Systems Interconnection - The Directory: Models, 1997.

## 7. Changes to Annex B

This module replaces the module in Annex B of [\[RFC3281\]](#). It incorporates verified technical errata #302 and #1480 and verified editorial errata #303.

Turner, et al.

Expires April 26, 2009

[Page 5]

---

Internet-Draft      Update: An Internet Attribute Certificate      Oct 2008

```
PKIXAttributeCertificate-2008 { iso(1) identified-organization(3)
  dod(6) internet(1) security(5) mechanisms(5) pkix(7) id-mod(0)
  id-mod-attribute-cert2(TBA) }
```

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

-- EXPORTS ALL --

IMPORTS

-- IMPORTed module OIDs MAY change if [\[PKIXPROF\]](#) changes  
-- PKIX Certificate Extensions

```
Attribute, AlgorithmIdentifier, CertificateSerialNumber,
Extensions, UniqueIdentifier, id-pkix, id-pe, id-kp, id-ad, id-at
FROM PKIX1Explicit88
  { iso(1) identified-organization(3) dod(6) internet(1)
    security(5) mechanisms(5) pkix(7) id-mod(0)
    id-pkix1-explicit-88(1) }
```

GeneralName, GeneralNames, id-ce

```

FROM PKIX1Implicit88
  { iso(1) identified-organization(3) dod(6) internet(1)
    security(5) mechanisms(5) pkix(7) id-mod(0)
    id-pkix1-implicit-88(2) }

;

id-pe-ac-auditIdentity      OBJECT IDENTIFIER ::= { id-pe 4 }
id-pe-aaControls            OBJECT IDENTIFIER ::= { id-pe 6 }
id-pe-ac-proxying          OBJECT IDENTIFIER ::= { id-pe 10 }
id-ce-targetInformation     OBJECT IDENTIFIER ::= { id-ce 55 }
id-aca                     OBJECT IDENTIFIER ::= { id-pkix 10 }
id-aca-authenticationInfo  OBJECT IDENTIFIER ::= { id-aca 1 }
id-aca-accessIdentity       OBJECT IDENTIFIER ::= { id-aca 2 }
id-aca-chargingIdentity     OBJECT IDENTIFIER ::= { id-aca 3 }
id-aca-group                OBJECT IDENTIFIER ::= { id-aca 4 }

```

```

-- { id-aca 5 } is reserved

id-aca-encAttrs             OBJECT IDENTIFIER ::= { id-aca 6 }
id-at-role                  OBJECT IDENTIFIER ::= { id-at 72}
id-at-clearance             OBJECT IDENTIFIER ::= {
  joint-iso-ccitt(2) ds(5) module(1) selected-attribute-types(5)
  clearance (55) }

-- Uncomment this if using a 1988 level ASN.1 compiler

-- UTF8String ::= [UNIVERSAL 12] IMPLICIT OCTET STRING

AttributeCertificate ::= SEQUENCE {
  acinfo          AttributeCertificateInfo,
  signatureAlgorithm AlgorithmIdentifier,
  signatureValue   BIT STRING
}

```

```

}

AttributeCertificateInfo ::= SEQUENCE {
    version                AttCertVersion, -- version is v2
    holder                 Holder,
    issuer                 AttCertIssuer,
    signature              AlgorithmIdentifier,
    serialNumber           CertificateSerialNumber,
    attrCertValidityPeriod AttCertValidityPeriod,
    attributes             SEQUENCE OF Attribute,
    issuerUniqueID         UniqueIdentifier OPTIONAL,
    extensions             Extensions OPTIONAL
}

AttCertVersion ::= INTEGER { v2(1) }

Holder ::= SEQUENCE {
    baseCertificateID  [0] IssuerSerial OPTIONAL,
        -- the issuer and serial number of
        -- the holder's Public Key Certificate
    entityName         [1] GeneralNames OPTIONAL,
        -- the name of the claimant or role
    objectDigestInfo   [2] ObjectDigestInfo OPTIONAL
        -- used to directly authenticate the
        -- holder, for example, an executable
}

```

```

ObjectDigestInfo ::= SEQUENCE {
    digestedObjectType  ENUMERATED {
        publicKey          (0),
        publicKeyCert      (1),
        otherObjectTypes   (2) },
        -- otherObjectTypes MUST NOT
        -- MUST NOT be used in this profile
    otherObjectTypeID   OBJECT IDENTIFIER OPTIONAL,
    digestAlgorithm     AlgorithmIdentifier,
    objectDigest        BIT STRING
}

AttCertIssuer ::= CHOICE {

```



```

    v1Form      GeneralNames, -- MUST NOT be used in this
                                -- profile
    v2Form [0] V2Form          -- v2 only
}

V2Form ::= SEQUENCE {
    issuerName      GeneralNames OPTIONAL,
    baseCertificateID [0] IssuerSerial OPTIONAL,
    objectDigestInfo [1] ObjectDigestInfo OPTIONAL
    -- issuerName MUST be present in this profile
    -- baseCertificateID and objectDigestInfo MUST
    -- NOT be present in this profile
}

IssuerSerial ::= SEQUENCE {
    issuer      GeneralNames,
    serial      CertificateSerialNumber,
    issuerUID   UniqueIdentifier OPTIONAL
}

AttCertValidityPeriod ::= SEQUENCE {
    notBeforeTime GeneralizedTime,
    notAfterTime  GeneralizedTime
}

Targets ::= SEQUENCE OF Target

Target ::= CHOICE {
    targetName [0] GeneralName,
    targetGroup [1] GeneralName,
    targetCert [2] TargetCert
}

```

```

TargetCert ::= SEQUENCE {
    targetCertificate IssuerSerial,
    targetName       GeneralName OPTIONAL,
    certDigestInfo   ObjectDigestInfo OPTIONAL
}

IetfAttrSyntax ::= SEQUENCE {
    policyAuthority [0] GeneralNames OPTIONAL,

```

```

values          SEQUENCE OF CHOICE {
                  octets  OCTET STRING,
                  oid     OBJECT IDENTIFIER,
                  string  UTF8String
                }
}

SvceAuthInfo ::= SEQUENCE {
  service  GeneralName,
  ident    GeneralName,
  authInfo OCTET STRING OPTIONAL
}

RoleSyntax ::= SEQUENCE {
  roleAuthority  [0] GeneralNames OPTIONAL,
  roleName       [1] GeneralName
}

Clearance ::= SEQUENCE {
  policyId          OBJECT IDENTIFIER,
  classList          ClassList DEFAULT {unclassified},
  securityCategories SET OF SecurityCategory OPTIONAL
}

ClassList ::= BIT STRING {
  unmarked      (0),
  unclassified  (1),
  restricted     (2),
  confidential  (3),
  secret        (4),
  topSecret     (5)
}

SecurityCategory ::= SEQUENCE {
  type  [0] OBJECT IDENTIFIER,
  value [1] EXPLICIT ANY DEFINED BY type
}

```

```

AAControls ::= SEQUENCE {
  pathLenConstraint  INTEGER (0..MAX) OPTIONAL,
  permittedAttrs     [0] AttrSpec OPTIONAL,

```

```
    excludedAttrs      [1] AttrSpec OPTIONAL,  
    permitUnspecified   BOOLEAN DEFAULT TRUE  
}
```

AttrSpec ::= SEQUENCE OF OBJECT IDENTIFIER

```
ACClearAttrs ::= SEQUENCE {  
    acIssuer  GeneralName,  
    acSerial  INTEGER,  
    attrs     SEQUENCE OF Attribute  
}
```

ProxyInfo ::= SEQUENCE OF Targets

END

## [8.](#) Security Considerations

The security considerations in [\[RFC3281\]](#) apply. No new security considerations are added as a result of this document.

## [9.](#) IANA Considerations

This document makes extensive use of object identifiers to register extensions and attributes. Most are registered in an arc delegated by IANA to the PKIX Working Group. Other are taken from ITU-T | ISO arc. Additionally, an object identifier is used to identify the ASN.1 module found in [Section 7](#). No further action by IANA is necessary for this document or any anticipated updates.

## [10.](#) References

### [10.1.](#) Normative

[PKIXPROF] 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](#), May 2008.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.

[RFC3281] Farrell, S., and R. Housley, "An Internet Attribute Certificate Profile for Authorization", [RFC 3281](#), April 2002.

[X.501-1997] ITU-T Recommendation X.501: Information Technology - Open Systems Interconnection - The Directory: Models, 1997.

## 10.2. Informative

None.

### Author's Addresses

Sean Turner

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

Email: [turners@ieca.com](mailto:turners@ieca.com)

Russ Housley

Vigil Security, LLC  
918 Spring Knoll Drive  
Herndon, VA 20170  
USA

Email: [housley@vigilsec.com](mailto:housley@vigilsec.com)

Stephen Farrell

Distributed Systems Group  
Computer Science Department  
Trinity College Dublin  
Ireland

Email: [stephen.farrell@cs.tcd.ie](mailto:stephen.farrell@cs.tcd.ie)

---

Internet-Draft      Update: An Internet Attribute Certificate      Oct 2008

## Full Copyright Statement

Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

## Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at [ietf-ipr@ietf.org](mailto:ietf-ipr@ietf.org).

## Acknowledgment

Funding for the RFC Editor function is provided by the IETF

Administrative Support Activity (IASA).

Turner, et al.

Expires April 26, 2009

[Page 12]