

Internet Draft  
PKIX Working Group  
February 2006  
Expires: August 2006

C. Francis  
Raytheon  
D. Pinkas  
Bull

Attribute Certificate Policies extension  
<[draft-ietf-pkix-acpolicies-extn-08.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>.

#### Copyright Notice

Copyright (C) The Internet Society (2006). All Rights Reserved.

#### Abstract

This document describes one certificate extension to explicitly state the Attribute Certificate Policies (ACPs) that apply to a given Attribute Certificate (AC). The goal of this document is to allow relying parties to perform an additional test when validating an AC, i.e. to assess whether a given AC carrying some attributes can be accepted on the basis of references to one or more specific ACPs.

#### Conventions Used In This Document

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 [[RFC 2119](#)].

Francis, Pinkas  
Internet-Draft

AC Policies extension

Page 1  
February 2006

## **1. Introduction**

When issuing a Public Key Certificate (PKC), a Certificate Authority (CA) can perform various levels of verification with regard to the subject identity (see [[RFC 3280](#)]). A CA makes its verification procedures, as well as other operational rules it abides by, "visible" through a certificate policy, which may be referenced by a certificate policies extension in the PKC.

The purpose of this document is to define an AC policies extension able to explicitly state the AC policies that apply to a given AC, but not the AC policies themselves. Attribute Certificates are defined in [[RFC 3281](#)].

## **2. AC Policies Extension Semantics**

An Attribute Certificate Policy is a named set of rules that indicates the applicability of an AC to a particular community and/or class of application with common security requirements and which defines rules for the generation, issuance and revocation of ACs. It may also include additional rules for attributes registration.

It should thus be noticed that an Attribute Authority (AA) does not necessarily support one single ACP. However, for each AC that is delivered the AA SHALL make sure that the policy applies to all the attributes that are contained in it.

An ACP may be used by an AC user to decide whether or not to trust the attributes contained in an AC for a particular purpose.

When an AC contains an AC policies extension, the extension MAY, at the option of the AA, be either critical or non-critical.

The AC Policies extension MAY be included in an AC. Like all X.509 certificate extensions [[X.509](#)], the AC policies extension is defined using ASN.1 [[ASN1](#)]. See Annex A.

The definitions are presented in the 1988 Abstract Syntax Notation One (ASN.1) rather than the 1997 ASN.1 syntax used in the most recent ISO/IEC/ITU-T standards.

The AC policies extension is identified by id-pe-acPolicies.



AcPolicyId ::= OBJECT IDENTIFIER

PolicyQualifierInfo ::= SEQUENCE {  
    policyQualifierId PolicyQualifierId,  
    qualifier ANY DEFINED BY policyQualifierId }

-- policyQualifierIds for Internet policy qualifiers

id-qt OBJECT IDENTIFIER ::= { id-pkix 2 }  
id-qt-acps OBJECT IDENTIFIER ::= { id-qt 4 }  
id-qt-acunotice OBJECT IDENTIFIER ::= { id-qt 5 }

id-qt-acps OBJECT IDENTIFIER ::= { iso(1)  
    identified-organization(3) dod(6) internet(1) security(5)  
    mechanisms(5) id-pkix(7) id-qt(2) 4 }

Francis, Pinkas  
Internet-Draft

AC Policies extension

Page 3  
February 2006

id-qt-acunotice OBJECT IDENTIFIER ::= { iso(1)  
    identified-organization(3) dod(6) internet(1) security(5)  
    mechanisms(5) id-pkix(7) id-qt(2) 5 }

PolicyQualifierId ::=  
    OBJECT IDENTIFIER ( id-qt-acps | id-qt-acunotice )

-- ACPS pointer qualifier

ACPSuri ::= IA5String  
-- ACP statement user notice qualifier

ACUserNotice ::= UserNotice  
-- UserNotice is defined in [[RFC3280](#)]

To promote interoperability, this document RECOMMENDS that policy information terms consist of only an OID. When more than one policy is used, the policy requirements have to be non-conflicting, e.g. one policy may refine the general requirements mandated by another policy.

The extension defined in this specification supports two policy qualifier types for use by ACP writers and AAs. The qualifier types are the ACPS Pointer and the AC User.

Notice qualifiers.

The ACPS Pointer qualifier contains a pointer to an Attribute Certification Practice Statement (ACPS) published by the AA. The pointer is in the form of a URI. Processing requirements for this qualifier are a local matter.

The AC User Notice is intended for display to a relying party when an attribute certificate is used. The application software SHOULD display the AC User Notice of the AC. The AC User Notice is defined in [RFC3280]. It has two optional fields: the noticeRef field and the explicitText field.

The noticeRef field, if used, names an organization and identifies, by number, a particular textual statement prepared by that organization. For example, it might identify the organization's name and notice number 1. In a typical implementation, the application software will have a notice file containing the current set of notices for the AA; the application will extract the notice text from the file and display it. Messages MAY be multilingual, allowing the software to select the particular language message for its own environment.

An explicitText field includes the textual statement directly in the certificate. The explicitText field is a string with a maximum size of 200 characters.

Francis, Pinkas  
Internet-Draft

AC Policies extension

Page 4  
February 2006

If both the noticeRef and explicitText options are included in the one qualifier and if the application software can locate the notice text indicated by the noticeRef option, then that text SHOULD be displayed; otherwise, the explicitText string SHOULD be displayed.

## **2.2 Attribute Certificate Policies**

The scope of this document is not the definition of the detailed content of ACPs themselves, therefore specific policies are not defined in this document.

## **3. Security Considerations**

The ACP defined in this document applies for all the attributes that are included in one AC. AAs SHALL ensure that the ACP applies to all the attributes which are included in the ACs they issue.

Attributes may be dynamically grouped in several ACs. It should be observed that since an AC may be issued under more than one ACP, the attributes included in a given AC MUST be compliant with all the ACPs from that AC.

When verifying an AC, a relying party MUST determine that the AC was issued by a trusted AA and then has the appropriate policy.

Failure of AAs to protect their private keys will permit an attacker to masquerade as them, potentially generating false ACs or revocation status. Existence of bogus ACs and revocation status will undermine confidence in the system. If the compromise is detected, all ACs issued by the AA MUST be revoked.

Rebuilding after such a compromise will be problematic, so AAs are advised to implement a combination of strong technical measures (e.g., tamper-resistant cryptographic modules) and appropriate management procedures (e.g., separation of duties) to avoid such an incident.

Loss of an AA's private signing key may also be problematic. The AA would not be able to produce revocation status or perform AC renewal (i.e. the issue of a new AC with the same set of attributes with the same values, for the same holder, from the same AA but with a different validity period). AC issuers are advised to maintain secure backup for signing keys. The security of the key backup procedures is a critical factor in avoiding key compromise.

The availability and freshness of revocation status will affect the degree of assurance that should be placed in a long-lived AC. While long-lived ACs expire naturally, events may occur during its natural lifetime which negate the binding between the AC holder and the attributes. If revocation status is untimely or unavailable, the assurance associated with the binding is clearly reduced.

The binding between an AC holder and attributes cannot be stronger than the cryptographic module implementation and algorithms used to generate the signature. Short key lengths or weak hash algorithms will limit the utility of an AC. AAs are encouraged to note advances in cryptology so they can employ strong cryptographic techniques.

If an AC is tied to the holder's PKC using the `baseCertificateID` component of the Holder field and the PKI in use includes a rogue CA with the same issuer name specified in the `baseCertificateID` component, this rogue CA could issue a PKC to a malicious party, using the same issuer name and serial number as the proper holder's PKC. Then the malicious party could use this PKC in conjunction with the AC. This scenario SHOULD be avoided by properly managing and configuring the PKI so that there cannot be two CAs with the same name. Another alternative is to tie ACs to PKCs using the `publicKeyCert` type in the `ObjectDigestInfo` field. Failing this, AC verifiers have to establish (using other means) that the potential collisions cannot actually occur, for example,

the Certificate Policy Statements (CPSs) of the CAs involved may make it clear that no such name collisions can occur.

Implementers MUST ensure that following validation of an AC, only attributes that the issuer is trusted to issue are used in authorization decisions. Other attributes, which MAY be present MUST be ignored. AC verifiers SHALL support means of being provided with this information. The AA controls PKC extension (see [\[RFC 3281\]](#)) is one possibility, but is optional to implement. Configuration information is a likely alternative means, while out-of-bands means is also another means. This becomes very important if an AC verification application trusts more than one AC issuer.

#### **4. IANA Considerations**

The AC policies extension is identified by an object identifier (OID). The OID for the AC policies extension defined in this document was assigned from an arc delegated by the IANA to the PKIX Working Group.

No further action by the IANA is necessary for this document.

#### **5. References**

##### **5.1 Normative references**

- [ITU-T Rec. X.660 | ITU-T Recommendation Rec X.660 (1992)  
ISO/IEC 9834-1] | ISO/IEC 9834-1: 1993, Information  
technology - Open Systems Interconnection  
Procedures for the operation of OSI  
Registration Authorities: General procedures.
- [RFC3280] Certificate and Certificate Revocation List (CRL) Profile.  
R. Housley, W.Polk, W.Ford, and D. Solo. April 2002.

Francis, Pinkas  
Internet-Draft

AC Policies extension

Page 6  
February 2006

- [RFC3281] An Internet Attribute Certificate Profile for  
Authorization. S. Farrell S. and R. Housley. April 2002.
- [ASN1] X.680 - X.693 | ISO/IEC 8824: 1-4 Abstract Syntax  
Notation One (ASN.1).

##### **5.2 Informative reference**

- [X.509] ITU-T Recommendation X.509 (2000): Information Technology  
Open Systems Interconnections - The Directory:  
Public-key and Attribute Frameworks, March 2000

## Author's Addresses

Christopher S. Francis  
Raytheon  
1501 72nd Street North, MS 25  
St. Petersburg, Florida 33764  
Email: Chris\_S\_Francis@Raytheon.com

Denis Pinkas  
Bull  
Rue Jean Jaures  
78340 Les Clayes-sous-Bois  
FRANCE  
Email: Denis.Pinkas@bull.net

## Full Copyright Statement

Copyright (C) The Internet Society (2006).

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 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](#).

Francis, Pinkas  
Internet-Draft

AC Policies extension

Page 7  
February 2006

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).

#### Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.

```

AcPolicies { iso(1) identified-organization(3) dod(6)
    internet(1) security(5) mechanisms(5) pkix(7) id-mod(0)
    id-mod-ac-policies(26) }

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

-- EXPORTS ALL --

IMPORTS

-- Imports from RFC 3280 \[RFC3280\], Appendix A

    UserNotice
        FROM PKIX1Implicit88 { iso(1) identified-organization(3)
            dod(6) internet(1) security(5) mechanisms(5) pkix(7)
            id-mod(0) 19 }

    id-pkix, id-pe
        FROM PKIX1Explicit88 { iso(1) identified-organization(3)
            dod(6) internet(1) security(5) mechanisms(5) pkix(7)
            id-mod(0) 18 };

-- Locally defined OIDs

    -- policyQualifierIds for Internet policy qualifiers

    id-qt                OBJECT IDENTIFIER ::= { id-pkix 2 }
    id-qt-acps            OBJECT IDENTIFIER ::= { id-qt 4 }
    id-qt-acunotice       OBJECT IDENTIFIER ::= { id-qt 5 }

-- Attributes

    id-pe-acPolicies      OBJECT IDENTIFIER ::= { id-pe 15 }

    AcPoliciesSyntax ::= SEQUENCE SIZE (1..MAX) OF PolicyInformation

    PolicyInformation ::= SEQUENCE {
        policyIdentifier      AcPolicyId,
        policyQualifiers      SEQUENCE SIZE (1..MAX) OF
            PolicyQualifierInfo OPTIONAL }

    AcPolicyId ::= OBJECT IDENTIFIER

    PolicyQualifierInfo ::= SEQUENCE {
        policyQualifierId      PolicyQualifierId,
        qualifier              ANY DEFINED BY policyQualifierId }

```

```
PolicyQualifierId ::=  
    OBJECT IDENTIFIER          ( id-qt-acps | id-qt-acunotice )  
-- ACPS pointer qualifier
```

```
ACPSuri ::= IA5String  
-- ACP statement user notice qualifier
```

```
ACUserNotice ::= UserNotice  
-- UserNotice is defined in [RFC3280]
```

END

