Groupe de travail Réseau
Request for Comments : 4476

Catégorie : Sur la voie de la normalisation

C. Francis, Raytheon
D. Pinkas, Bull
mai 2006
Traduction Claude Brière de L'Isle

Extension des politiques de certificat d'attribut (AC)

Résumé
Le présent document décrit une extension de certificat qui déclare explicitement les politiques de certificat d'attribut (ACP, *Attribute Certificate Policy*) qui s'appliquent à un certain certificat d'attribut (CA, *Attribute Certificate*). Le but de ce document est de permettre aux parties d'effectuer une vérification supplémentaire lors de la validation d'un AC, c'est-à-dire, d'affirmer si un certain AC portant des attributs peut être accepté sur la base des références à une ou plusieurs ACP spécifiques.

1. Introduction

Quand elle produit un certificat de clé publique (PKC, *Public Key Certificate*) une autorité de certification (CA, *Certificate Authority*) peut effectuer divers niveaux de vérification à l'égard de l'identité du sujet (voir la [RFC3280]). Une CA rend "visibles" ses procédures de vérification, ainsi que les autres règles opérationnelles auxquelles elle se conforme, à travers une politique de certificat, qui peut être référencée par une extension de politiques de certificat dans le PKC.

L'objet du présent document est de définir une extension des politiques de certificat d'attribut (AC) capable de déclarer explicitement les politiques d'AC qui s'appliquent à un certain AC, mais non les politiques d'AC elles-mêmes. Les certificats d'attributs sont définis dans la [RFC3281].

1.1 Conventions utilisées dans le document

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

2. Sémantique de l'extension Politiques d'AC

Une politique de certificat d'attribut est un ensemble désigné de règles qui indiquent l'applicabilité d'un AC à une communauté et/ou classe d'applications particulière avec des exigences de sécurité communes. Elle définit des règles pour la génération, la production, et la révocation des AC. Elle peut aussi inclure des règles supplémentaires pour l'enregistrement des attributs.

Donc, on note qu'une autorité d'attribut (AA, *Attribute Authority*) ne prend pas nécessairement en charge une seule ACP. Cependant, pour chaque AC qui est livré, la AA DEVRA s'assurer que la politique s'applique à tous les attributs qu'elle contient.

Une ACP peut être utilisée par un utilisateur d'AC pour décider de faire confiance ou non aux attributs contenus dans un AC pour un objet particulier.

Quand un AC contient une extension de politiques d'AC, l'extension PEUT, au choix de l'AA, être critique ou non critique.

L'extension de politiques d'AC PEUT être incluse dans un AC. Comme toutes les extensions de certificat X.509 [X.509], l'extension de politiques d'AC est définie en utilisant la notation ASN.1 [ASN1]. Voir l'Appendice A.

Les définitions sont présentées dans la notation de syntaxe abstraite numéro un de 1988 (ASN.1, *Abstract Syntax Notation One*) plutôt que dans la syntaxe ASN.1 de 1997 utilisée dans les normes les plus récentes de l'ISO/CEI/UIT-T.

L'extension de politiques d'AC est identifiée par id-pe-acPolicies.

IDENTIFIANT D'OBJET id-pe-acPolicies ::= { iso(1) identified-organization(3) dod(6) internet(1) security(5)
mechanisms(5) id-pkix(7) id-pe(1) 15 }

L'extension de politiques d'AC inclut une liste des politiques d'AC reconnues par l'AA qui applique les attributs inclus dans l'AC.

Les politiques d'AC peuvent être définies par toute organisation qui en a besoin. Les identifiants d'objet utilisés pour identifier les politiques d'AC sont alloués conformément à [X.660].

L'extension de politiques d'AC dans un AC indique les politiques d'AC pour lesquelles l'AC est valide.

Une application qui reconnaît cette extension et son contenu DEVRA traiter l'extension sans considération de la valeur du fanion de criticité.

Si l'extension est à la fois marquée non critique et non reconnue par l'application qui utilise l'AC, l'application PEUT l'ignorer.

Si l'extension est marquée comme critique ou est reconnue par l'application qui utilise l'AC, cela indique que les attributs contenus dans le certificat d'attribut DEVRONT seulement être utilisés pour l'objet, et en accord avec les règles associées à une des politiques d'AC indiquées. Si aucun des identifiants d'ACP n'est adéquat pour l'application, l'AC DOIT alors être rejeté.

Si l'extension est marquée comme critique ou est reconnue par l'application qui utilise l'AC, celle-ci DOIT utiliser la liste des politiques d'AC pour déterminer si elles sont appropriées pour utiliser les attributs contenus dans cet AC pour une certaine transaction. Quand la politique appropriée n'est pas trouvée, l'AC DEVRA être rejeté.

2.1 Syntaxe d'extension de politique d'AC

La syntaxe de l'extension de politique d'AC est :

```
AcPoliciesSyntax ::= TAILLE DE SEQUENCE (1..MAX) DE PolicyInformation

PolicyInformation ::= SEQUENCE {
     policyIdentifier     AcPolicyId,
     policyQualifiers      TAILLE DE SEQUENCE (1..MAX) DE PolicyQualifierInfo FACULTATIF}

PolicyQualifierInfo ::= SEQUENCE {
       policyQualifierId  PolicyQualifierId,
       qualifier              TOUS DEFINIS PAR policyQualifierId }

-- policyQualifierIds pour qualificatifs de politique Internet

IDENTIFIANT D'OBJET id-qt ::=  { id-pkix 2 }
IDENTIFIANT D'OBJET id-qt-acps ::=  { id-qt 4 }
IDENTIFIANT D'OBJET id-qt-acunotice ::=  { id-qt 5 }

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

IDENTIFIANT D'OBJET id-qt-acunotice ::= { iso(1) identified-organization(3) dod(6) internet(1) security(5)
```

mechanisms(5) id-pkix(7) id-qt(2) 5 }

PolicyQualifierId ::= IDENTIFIANT D'OBJET (id-qt-acps | id-qt-acunotice)

-- qualificatif de pointeur ACPS

ACPSuri ::= IA5String
-- qualificatif de notice d'utilisateur de déclaration d'ACP

ACUserNotice ::= UserNotice
-- UserNotice est défini dans la [RFC3280]

Pour promouvoir l'interopérabilité, le présent document RECOMMANDE que les termes d'informations de politique consistent seulement en un identifiant d'objet (OID, *object identifier*). Quand plus d'une politique est utilisée, les exigences de politique doivent être non conflictuelles, par exemple, une politique peut préciser les exigences générales rendues obligatoires par une autre politique.

L'extension définie dans cette spécification prend en charge deux types de qualificatifs de politique à utiliser par les rédacteurs d'ACP et les AA. Les types de qualificatifs sont le pointeur ACPS et l'utilisateur d'AC.

2.1.1 Qualificatifs de notice

Le qualificatif pointeur ACPS contient un pointeur sur une déclaration de pratique de certification d'attribut (ACPS, *Attribute Certification Practice Statement*) publiée par le AA. Le pointeur est sous forme d'URI. Les exigences de traitement pour ce qualificatif sont une affaire locale.

La notice d'utilisateur d'AC est destinée à être affichée au consommateur d'assertion quand un certificat d'attribut est utilisé. Le logiciel d'application DEVRAIT afficher la notice d'utilisateur d'AC de l'AC. La notice d'utilisateur d'AC est définie dans la [RFC3280]. Elle a deux champs facultatifs : le champ noticeRef et le champ explicitText.

Le champ noticeRef, s'il est utilisé, désigne une organisation et identifie, par un numéro, une déclaration textuelle particulière préparée par cette organisation. Par exemple, il peut identifier le nom de l'organisation et la notice numéro 1. Dans une mise en œuvre normale, le logiciel d'application va avoir un fichier de notices contenant l'ensemble actuel de notices pour l'AA ; l'application va extraire le texte de la notice du fichier et l'afficher. Les messages PEUVENT être en plusieurs langues, permettant au logiciel de choisir le message dans la langue particulière de son propre environnement.

Un champ explicitText inclut la déclaration textuelle directement dans le certificat. Le champ explicitText est une chaîne d'une taille maximum de 200 caractères.

Si les deux options noticeRef et explicitText sont incluses dans le qualificatif, et si le logiciel d'application peut localiser le texte de la notice indiquée par l'option noticeRef, alors ce texte DEVRAIT être affiché ; autrement, la chaîne explicitText DEVRAIT être affichée.

2.2 Politiques de certificat d'attribut

Le domaine d'application du présent document n'est pas la définition du contenu détaillé des ACP eux-mêmes ; donc, les politiques spécifiques ne sont pas définies dans ce document.

3. Considérations sur la sécurité

L'ACP défini dans le présent document s'applique pour tous les attributs qui sont inclus dans un AC. Les AA DEVRONT s'assurer que l'ACP s'applique à tous les attributs qui sont inclus dans les AC qu'elles produisent.

Les attributs peuvent être groupés dynamiquement dans plusieurs AC. Il devrait être observé que comme un AC peut être produit sous plus d'une ACP, les attributs inclus dans un certain AC DOIVENT être conformes avec toutes les ACP provenant de cet AC.

Lors de la vérification d'un AC, un consommateur d'assertions DOIT déterminer si l'AC a été produit par une AA de

confiance et ensuite qu'il a la politique appropriée.

L'échec des AA à protéger leurs clés privées va permettre à un attaquant de se faire passer pour elles, générant potentiellement de faux AC ou statuts de révocation. L'existence d'AC et de statuts de révocation fallacieux va miner la confiance dans le système. Si la compromission est détectée, alors le certificat de l'AA DOIT être révoqué.

La reconstruction après une telle compromission sera problématique, donc il est conseillé aux AA de mettre en œuvre une combinaison de fortes mesures techniques (par exemple, des modules de chiffrement résistants à l'altération) et de procédures de gestion appropriées (par exemple, la séparation des tâches) pour éviter de tels incidents.

La perte d'une clé de signature privée d'un AA peut aussi être problématique. L'AA ne sera pas capable de produire un statut de révocation ou d'effectuer un renouvellement d'AC (c'est-à-dire, la production d'un nouvel AC avec le même ensemble d'attributs des mêmes valeurs, pour le même détenteur, à partir de la même AA mais avec une période de validité différente). Il est conseillé aux producteurs d'AC de conserver des sauvegardes sécurisées pour les clés de signature. La sécurité des procédures de sauvegarde de clés est un facteur critique pour éviter la compromission des clés.

La disponibilité et la fraîcheur du statut de révocation va affecter le degré d'assurance qui devrait être porté à un AC de longue durée. Bien que les AC de longue durée arrivent naturellement à expiration, des événements peuvent se produire durant la vie normale d'un AC qui rompent le lien entre le détenteur de l'AC et les attributs. Si le statut de révocation n'intervient pas à temps ou est indisponible, l'assurance associée au lien est clairement réduite.

Le lien entre un détenteur d'AC et les attributs ne peut pas être plus fort que la mise en œuvre du module cryptographique et des algorithmes utilisés pour générer la signature. Les courtes longueurs de clé ou des algorithmes de hachage faibles vont limiter l'utilité d'un AC. Les AA sont invitées à noter les avancées en cryptologie afin qu'elles puissent employer des techniques cryptographiques fortes.

Si un AC est lié au PKC du détenteur en utilisant le composant baseCertificateID du champ Holder et si la PKI utilisée inclut un CA falsifié avec le même nom de producteur que spécifié dans le composant baseCertificateID, ce CA falsifié pourrait produire un PKC à une partie malveillante, en utilisant le même nom de producteur et le même numéro de série que le PKC du propre détenteur. Alors la partie malveillante pourrait utiliser ce PKC en conjonction avec l'AC. Ce scénario DEVRAIT être évité en gérant de façon appropriée et en configurant la PKI de telle sorte qu'il ne puisse y avoir deux CA avec le même nom. Une autre solution est de lier les AC aux PKC en utilisant le type publicKeyCert dans le champ ObjectDigestInfo. Faute de quoi, les vérificateurs d'AC devront établir (en utilisant d'autres moyens) que des collisions potentielles ne peuvent en fait pas se produire ; par exemple, les déclarations de politique de certificat (CPS, *Certificate Policy Statement*) des CA impliqués peuvent rendre clair qu'aucune collision de noms ne peut se produire.

Les mises en œuvre DOIVENT s'assurer qu'à la suite de la validation d'un AC, seuls les attributs dont le producteur est de confiance pour les produire sont utilisés dans les décisions d'autorisation. Les autres attributs, qui PEUVENT être présents, DOIVENT être ignorés. Les vérificateurs d'AC DEVRONT prendre en charge les moyens d'en être informés. L'extension PKC de contrôle d'AA (voir la [RFC3281]) est une possibilité, mais sa mise en œuvre est facultative. Les informations de configuration sont probablement un moyen de remplacement, tandis que des moyens hors bande en sont un autre. Cela devient très important si une application de vérification d'AC fait confiance à plus d'un producteur d'AC.

4. Considérations relatives à l'IANA

L'extension Politiques d'AC est identifiée par un identifiant d'objet (OID). L'OID pour l'extension Politiques d'AC définie dans le présent document a été alloué dans un arc délégué par l'IANA au groupe de travail PKIX.

Aucune autre action de l'IANA n'est nécessaire pour le présent document.

5. Références

5.1 Références normatives

[ASN1] Recommandations UIT-T X.680 - X.693 | ISO/CEI 8824: 1-4 "Notation de syntaxe abstraite numéro un (ASN.1)".

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997.

(MàJ par RFC8174)

[RFC3280] R. Housley, W. Polk, W. Ford et D. Solo, "Profil de certificat d'infrastructure de clé publique X.509 et de liste de révocation de certificat (CRL) pour l'Internet", avril 2002. *(Obsolète, voir* RFC5280)

[RFC3281] S. Farrell et R. Housley, "Profil de certificat d'attribut Internet pour l'autorisation", avril 2002. *(Obsolète, voir* RFC5755)

[X.660] Recommandation UIT-T X.660| ISO/CEI 9834-1: 1993, "Technologie de l'information - Interconnexion des systèmes ouverts - Procédures pour le fonctionnement des autorités d'enregistrement OSI : procédures générales". (1992)

5.2 Références pour information

[X.509] Recommandation UIT-T X.509, "Technologie de l'information - Interconnexion des systèmes ouverts - L'annuaire : cadres de clé publique et d'attributs", mars 2000.

Appendice A Définitions ASN.1

Cet appendice est normatif.

Module ASN.1

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

ÉTIQUETTES DE DÉFINITIONS IMPLICITES ::=

DÉBUT

-- EXPORTE TOUT --

IMPORTE

-- Importe de la [RFC3280], Appendice A

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

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

-- OID définis localement

-- policyQualifierIds pour les qualificatifs de politique Internet

IDENTIFIANT D'OBJET id-qt  ::=  { id-pkix 2 }
IDENTIFIANT D'OBJET id-qt-acps ::=  { id-qt 4 }
IDENTIFIANT D'OBJET id-qt-acunotice ::=  { id-qt 5 }

-- Attributs

IDENTIFIANT D'OBJET id-pe-acPolicies ::= { id-pe 15 }

AcPoliciesSyntax ::= TAILLE DE  SEQUENCE (1..MAX) DE PolicyInformation
```

```
PolicyInformation ::= SEQUENCE {
    policyIdentifier    AcPolicyId,
    policyQualifiers    TAILLE DE SEQUENCE (1..MAX) DE PolicyQualifierInfo FACULTATIF }

IDENTIFIANT D'OBJET AcPolicyId ::= IDENTIFIANT D'OBJET

PolicyQualifierInfo ::=  SEQUENCE {
    policyQualifierId    PolicyQualifierId,
    qualifier              TOUT DEFINI PAR policyQualifierId }

PolicyQualifierId ::= IDENTIFIANT D'OBJET ( id-qt-acps | id-qt-acunotice )
-- qualificatif de pointeur ACPS

ACPSuri ::= IA5String
-- qualificatif de notice d'utilisateur de déclaration d'ACP

ACUserNotice ::=    UserNotice
-- UserNotice est défini dans la [RFC3280]

FIN
```

Adresse des auteurs

Christopher S. Francis
Raytheon
1501 72nd Street North, MS 25
St. Petersburg, Florida 33764
US
mél : Chris_S_Francis@Raytheon.com

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

Déclaration complète de droits de reproduction

droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf-ipr@ietf.org.

Remerciement
Le financement de la fonction d'édition des RFC est fourni par l'activité de soutien administatif (IASA) de l'IETF.