

<b>Statut du document</b>	<i>Standards Track</i>
<b>Titre</b>	<i>An Internet Attribute Certificate Profile for Authorization</i> RFC 3281 Profil de certificat d'attributs pour autorisation par Internet
<b>Mot clé</b>	Attestation et sécurité
<b>Source</b>	IETF <a href="ftp://ftp.rfc-editor.org/in-notes/rfc3281.txt">ftp://ftp.rfc-editor.org/in-notes/rfc3281.txt</a>
<b>Date de publication</b>	Avril 2002
<b>Nombre de pages</b>	40
<b>Langue</b>	Anglais
<b>Lien avec autres normes</b>	Fondé sur l'architecture PKIX de l'IETF et le certificat X.509. Alors que l'UIT, dans la version de 1988 et dans celle de 1997, avait limité son attention au cadre d'authentification, la version X.509 publiée en 2000 porte sur deux types de certificat : les certificats de clé publique et les certificats d'attribut.
<b>Situation actuelle</b>	Un document complémentaire de l'IETF, <i>Implementing Company Classification Policy with the S/MIME Security Label</i> , RFC 3114, fournit un aperçu général sur la manière de relier diverses normes ayant trait à la catégorisation des ressources informationnelles de façon à optimiser l'usage des moyens de protection, en particulier dans l'usage de S/MIME. Voir <a href="ftp://ftp.rfc-editor.org/in-notes/rfc3114.txt">ftp://ftp.rfc-editor.org/in-notes/rfc3114.txt</a>
<b>Description</b>	<p>Parce que la nouvelle version de la norme X.509 définit maintenant deux types de certificat, le terme <i>certificat X.509</i>, depuis longtemps en usage, désigne désormais deux types d'objet distincts :</p> <ul style="list-style-type: none"> <li>- le <u>certificat de clé publique</u> : attache ensemble une valeur de clé publique et une identité; analogue à un passeport (lequel suppose une vérification préalable d'identité).</li> <li>- le <u>certificat d'attribut</u> : attache ensemble une identité et des attributs servant à véhiculer des autorisations; analogue à un visa (lequel suppose une vérification de passeport).</li> </ul> <p>Dans la version antérieure de la norme, le certificat X.509 pouvait comporter des extensions permettant de véhiculer ces attributs. Cette forme d'usage a cependant été limitée parce qu'elle posait des problèmes de gestion d'information stables pour l'identité avec l'information plus changeante des attributs. C'est pourquoi les deux types de certificat ont été définis pour permettre un déploiement des solutions mieux adaptées aux exigences variables des contextes. Le certificat d'attribut contient donc une identité, elle-même établie avec un certificat de clé publique. Le client peut soit transmettre son certificat d'attribut au serveur, soit le voir demandé par le serveur à un autre serveur, qui est chargé de transmettre le certificat d'attribut pour cette identité certifiée. Un même certificat peut rassembler les attributs fournis par plusieurs autorités d'attribut distinctes.</p> <p>Le présent document de l'IETF vise à fournir des éléments structurels généraux pour faciliter l'usage des certificats d'attributs. Un profil d'éléments est fourni pour le définir. Il s'agit des éléments classiques de ce certificat, i.e. ceux qui portent sur le certificat, son émetteur, son détenteur et les attributs qui sont attachés à son identité.</p> <p>Des contraintes syntaxiques variées sont définies pour une meilleure interopérabilité dans le cadre architectural PKIX.</p>

	<p>Dans un certificat d'attribut, six types d'attribut sont possibles :</p> <ul style="list-style-type: none"> <li>- authentification d'information pour un service</li> <li>- identification pour l'accès</li> <li>- identification pour le paiement</li> <li>- appartenance à un Groupe</li> <li>- assignation d'un Rôle</li> <li>- autorisation (en anglais <i>clearance</i>) : tel que défini dans X.501 – 1993, six catégories sont définies : (0) sans indication, (1) non confidentiel, (2) protégé, (3) confidentiel, (4) secret, (5) très secret. Ces significations et ces valeurs de code ne peuvent être changées, toute précision supplémentaire pouvant être ajoutées en prenant une valeur de code de 6, 7 etc., et leur signification devant alors être retraçable dans la politique de sécurité pertinente.</li> </ul>
--	---

**Remarque**

Comparer avec les certificats d'autorisation SPKI, voir par exemple <http://www.autoroute.gouv.qc.ca/publica/normes/norme60.htm> Une différence importante pourrait être que SPKI recourt à un encodage XML alors qu'ici cet encodage est en ASN.1 dans sa partie *DER (Direct Encoding Rule)*, ce qui entraîne la nécessité d'une séquence stricte des éléments.

**Lexique anglais-français**

Attribute certificate	Certificat d'attribut
Clearance	Autorisation
Public key certificate	Certificat de clé publique
Restricted	Protégé
Top secret	Très secret
Unclassified	Non confidentiel (public)
Unmarked	Sans indication

**Rédacteur :** Richard Parent  
**Organisation source :** Secrétariat du Conseil du trésor  
**Date de publication :** 10 juillet 2002  
**Raison d'être :** Connaissance technologique  
**Programme gouvernemental :** Inforoutes et ressources informationnelles  
**Nom du modificateur :**  
**Date de dernière modification :**  
**Note numéro :** 131