

Statut du document	<i>Internet-Draft</i>
Titre	<i>XML Encoding of SPKI Certificates</i>
Mots clés	Attestation et sécurité
Source	IETF http://www.ietf.org/internet-drafts/draft-paajarvi-xml-spki-cert-00.txt
Date de publication	Mars 2000
Nombre de pages	30
Langue	Anglais
Liens avec autres normes	Représentation en XML du « certificat SPKI » défini dans RFC2692, RFC2693 (autre Note de lecture), ainsi que dans <i>Simple Public Key Certificate</i> , ce dernier à http://world.std.com/~cme/spki.txt
Situation courante	
Description	<p>Un certificat est une attache entre une clé servant à l'identification et des attributs comme le nom, des autorisations, etc. Les certificats SPKI, déjà définis selon l'encodage des s-expressions, peuvent être avantageusement représentés en structures XML. Le présent document présente une DTD de certificat d'autorisation, lequel est la forme de base pour les certificats SPKI.</p> <p>On a besoin de certificats dans une architecture de sécurité, mais ils sont trop complexes à déployer actuellement. Une part de cette complexité est attribuable à l'encodage des certificats X.509 en ASN.1 tandis que les certificats SPKI sont dans un encodage différent des s-expressions : aucun de ces deux encodages n'est courant dans l'Internet. D'où cette proposition d'encodage XML des certificats :</p> <ul style="list-style-type: none"> - pour le monde plus souple avec les cellulaires aussi pour transiger, - pour tirer profit des API que sont DOM et SAX dans le monde XML, - pour un passage régulier des certificats avec validation XML qui sera prochainement disponible sur tout serveur Web, - pour un format lisible par les humains en plus des ordinateurs, - pour un format aisément convertible en toute forme de représentation voulue grâce à XSL. <p>Seuls les certificats d'autorisation sont présentés en détail, mais des DTD sont aussi définies pour les certificats de nom, les certificats d'ACL (liste de contrôle d'accès), les certificats de CRL (listes de révocation de certificat), et les formats de réponse aux tests synchrones en réseau.</p> <p>Les objets primaires des certificats SPKI sont :</p> <ol style="list-style-type: none"> 1- Clé publique de type soit RSA, soit DSA. 2- Empreinte avec attribut obligatoire identifiant l'algorithme utilisé (<i>md5</i>, <i>sha1</i>, autre). 3- Empreinte de clé publique après qu'elle ait été régularisée (canonicalisée) conformément à <i>XMLdsig</i> pour obtenir un nom plus court utilisable en contexte. 4- <i>Uniform Resource Identifier</i> (URI) ou URL pointant sur une ressource dont le sens est clair en contexte. 5- Signature : la plupart des objets de certification requièrent des signatures numériques conformes à <i>XMLdsig</i>. <p>Le certificat d'autorisation est la forme fondamentale de certificat SPKI. Il sert à transférer une habilitation au moyen d'un certificat émis par un détenteur d'autorité au Sujet d'un certificat. Une demande est vérifiée via une chaîne de certification des autorisations, celle-là même qui avait auparavant transféré un certificat venant de l'émetteur racine jusqu'au sujet. L'émetteur racine est responsable d'élaborer sa liste de contrôle d'accès à la racine avec un modèle de structure de données définie dans</p>

	<p>une liste de contrôle d'accès, extrêmement secrète, qui institue les certificats racine, ceux qui n'ont ni émetteur, ni signature. Le certificat d'autorisation est composé d'un élément, cert, qui se définit comme ayant les sous-éléments suivants :</p> <p>1- <u>Version</u> : 0 par défaut désigne la présente spécification</p> <p>2- <u>Émetteur</u> : désigné par sa clé publique ou l'empreinte de celle-ci, et un URI facultatif de source de certification.</p> <p>3- <u>Sujet</u> : détenteur et bénéficiaire du certificat, entité habilitée par le certificat, il est désigné par une clé publique, ou une empreinte de clé publique, ou un nom, ou une empreinte d'objet.</p> <p>4- <u>Délégation</u> : Si le corps d'un certificat contient un élément de délégation, le sujet du certificat peut non seulement utiliser les permissions ou attributs transférés par le certificat, mais il a aussi la permission de les transférer à son tour, en totalité ou en partie, à d'autres.</p> <p>5- <u>Étiquette (tag)</u> : L'élément étiquette contient les attributs, autorisations, permissions, capacités, paramètres ou toute chose qu'un certificat peut transférer. L'élément doit donner un nom à chaque étiquette qu'il transfère. Il y a des problèmes à résoudre dans la réduction de deux certificats en un seul : certaines étendues et certains ensembles d'étiquettes sont exprimés de façon complexe et d'une façon qui est liée à leur application, comme c'est le cas des permissions Java.</p> <p>6- <u>Validité</u> : L'élément de validité indique quelles sont les contraintes devant être respectées pour que soit validé un certificat. Les contraintes les plus cruciales sont les dates « pas avant » et « pas après » qui devraient être obligatoires. Cet intervalle peut être restreint avec des tests synchrones en réseau qui peuvent interrompre la validité ou en rapprocher l'échéance. Il y a aussi un élément Nouveau certificat (<i>New-cert</i>) qui permet d'indiquer un URI pour obtenir un nouveau certificat dans des situations où ceux-ci ont des durées de vie réduites.</p> <p>7- <u>Commentaire</u> : Zone facultative pour insérer un message pour lecture humaine.</p> <p>Un certificat de nom, un certificat d'une entrée de liste de contrôle d'accès, un certificat relatif à la révocation, un certificat de revalidation, un certificat de revalidation une-fois : ces DTD sont esquissées en référence à la présentation dans qui en a été faite dans SPKI (juillet 1999). Une solution particulière est aussi proposée pour associer les permissions Java sans compromettre la validité.</p>
--	---

Remarques

Lexique anglais-français

Access Control List (ACL)	Liste de contrôle d'accès	Liste d'entrées qui fournit un point d'ancrage à une chaîne de certificat. Parfois appelé « liste des clés racine », la liste de contrôle d'accès est la source d'habilitation pour les certificats (de l'émetteur au sujet). L'entrée a le même contenu qu'un certificat, sauf pour l'identification de l'émetteur et sa signature.
Base64	Base64	Une méthode d'encodage pour convertir entre une représentation en ASCII (caractères) et une représentation en binaire. Définie dans RFC2045.
Certificate	Certificat	Un instrument signé qui habilite le sujet. Contient au moins un Émetteur et un Sujet. Peut contenir des conditions de validité, des renseignements d'autorisation et de délégation. Il y en a

		trois catégories: ID (nom, clé), Attribut (autorisation, nom), et Autorisation (autorisation, clé). Ce qui identifie le plus directement un individu, ce n'est pas son nom mais sa clé.
Fully Qualified Name	Nom pleinement qualifié	Un nom local adjoint à un identifiant global qui définit l'espace nominatif local.
Global Identifier	Identifiant global	Une chaîne d'octets globalement unique, associée au détenteur de clé. Dans SPKI, il s'agit de la clé publique elle-même, d'une empreinte de la clé publique ou d'un Nom pleinement qualifié.
Hash	Calcul d'empreinte	Une fonction de calcul d'empreinte cryptographiquement forte. En général l'empreinte d'un objet peut être utilisée partout où l'objet peut apparaître. L'empreinte sert de nom à l'objet à partir duquel elle a été « prise » (calculée).
Issuer	Émetteur	Le signataire d'un certificat et la source d'habilitation que le certificat communique au Sujet.
Keyholder	Détenteur de clé	La personne ou autre entité qui détient et contrôle une clé privée donnée. Cette entité est considérée détentrice de la biclé, ou juste de la clé publique, mais le contrôle de la clé privée est pris pour acquis dans tous les cas.
Name	Nom	Un nom SDSI toujours relatif au définisseur d'un espace nominatif. On le désigne aussi comme un nom local, qui n'est pas pleinement qualifié, i.e. sans identifiant global.
Online Test	Test synchrone en réseau	Test de validation d'un certificat grâce à une validation demandée en réseau et dont la réponse est obtenue immédiatement. Une des trois formes possibles : 1) liste de certificats révoqués; 2) revalidation; 3) revalidation une-fois . Chaque validation rétrécit la période temporelle de validité qui est spécifiée.
Principal	Titre	Une clé cryptographique, capable de générer une signature numérique. Note : en droit, un titre est un acte écrit, une pièce authentique qui sert à établir un droit, une qualité.
Prover	Demandeur	L'entité qui demande un accès ou qui signe numériquement un document. Généralement le demandeur envoie un message ou ouvre un canal au Vérificateur qui valide alors les signatures et attestations envoyées par le demandeur. Note : alors que <i>Prover</i> met l'accent sur la preuve présentée, <i>demandeur</i> met l'accent sur celui qui demande à être reconnu.
s-expression	s-expression	Le format de donnée choisi pour SPKI/SDSI, il s'agit d'un genre d'expression avec parenthèses emboîtées de façon semblable au langage Lisp.
Speaking	Parle	On dit qu'un titre « parle » au moyen d'une signature numérique. L'énoncé qui est produit est l'objet signé, souvent un certificat. Le titre parle au nom du détenteur de clé.
Subject	Sujet	La chose qui se trouve habilitée par un certificat ou une entrée de liste de contrôle d'accès. Ça peut être sous forme d'une clé, d'un nom (associé par certificat à une clé ou un objet), d'une empreinte de quelque objet, ou d'un ensemble de clés arrangées dans une fonction avec seuils (<i>threshold function</i>).

Threshold Subject	Sujet avec seuils	Un Sujet pour une entrée de liste de contrôle d'accès ou un certificat qui spécifie K de N autres Sujets. Conceptuellement, l'habilitation transmise au Sujet par l'entrée ou le certificat est transmis en quantité de 1/K à chaque Sujet subordonné listé. K de ces Sujets subordonnés doivent se mettre d'accord pour concentrer la délégation de leur part sur un même objet ou clé pour que l'habilitation puisse être effectuée. Ce mécanisme introduit de la robustesse et aide à protéger les clés racine.
Tuple	Tuple	Nombre de parties d'une unité, par analogie avec <i>quintuple</i> , <i>centuple</i> , en l'appliquant aux champs qui, dans un certificat ou une entrée de liste de contrôle d'accès, ont trait à la sécurité. On parle d'un 4-tuple pour un certificat de nom (Émetteur, Nom, Sujet, Validité), et d'un 5-tuple pour les autorisations (Émetteur, Sujet, Délégation, Autorisation, Validité).
Validity conditions	Conditions de validité	Une période de calendrier qui doit inclure le moment actuel et/ou des tests de validation qui doivent être réussis avant qu'un certificat voit reconnaître sa validité.
Verifier	Vérificateur	L'entité qui traite les requêtes des demandeurs, y compris les certificats. Le Vérificateur utilise ses propres entrées de liste de contrôle d'accès en plus des certificats fournis par le Demandeur pour effectuer une « réduction à un 5-tuple » de ce qu'il croit à propos du Demandeur (Soi (<i>self</i>), demandeur, D, A, V)

Rédacteur : Richard Parent
Organisation source : Secrétariat du Conseil du trésor
Date de publication : 21 août 2000
Raison d'être : Connaissance technologique
Programme gouvernemental : Inforoutes et ressources informationnelles
Nom du modificateur : Richard Parent
Date de dernière modification : 27 mars 2002
Note numéro : 60