

Statut du document	Proposition ouverte
Titre	<i>Trust Policy Language (TPL)</i> . Langage de politique de confiance
Mot clé	Attestation et sécurité
Source	IBM
Date de publication	Janvier 2000
Nombre de pages	6
Langue	Anglais
Lien avec autres normes	Basé sur XML en associant les concepts du contrôle d'accès à base de rôles.
Situation actuelle	
Description	<p>Une façon reconnue de simplifier le contrôle d'accès aux ressources en réseau est de modéliser des rôles pour regrouper les stéréotypes d'autorisations et pour pouvoir ensuite assigner ces rôles aux utilisateurs. Cela permet de réduire considérablement le nombre de décisions de contrôle d'accès imposées au système. De plus en plus, les mots de passe sont remplacés par un protocole d'authentification comme SSL qui vérifie que l'utilisateur dispose de la clé privée qu'il prétend avoir. Traditionnellement, la conception s'est souvent bornée à cette question d'identité à établir, mais ça s'avère incomplet dès que la réponse doit être plus raffinée qu'un simple oui/non global. Avec les réseaux ouverts, le besoin d'échanges plus faciles au niveau des autorisations certifiées devient plus pressant que jamais.</p> <p>PGP et SPKI se situent dans cet axe d'évolution poursuivi par TPL. L'accent se déplace vers un certificat signé par un émetteur crédible à propos d'un « sujet » qui détient une clé publique et qui a tels attributs, rôles, autorisations, etc. Une structure de référence XML de « certificat TE » (<i>Trust Establishment</i>) est proposée afin de permettre l'interopérabilité entre des produits variés comme X.509v.3, SPKI, PGP, KeyNote. Des types (sémantiques) de certificats et leurs structures différentes pourront être établis pour faciliter le traitement. Les politiques elles-mêmes doivent être traitables automatiquement pour répondre aux exigences du commerce électronique.</p> <p>Les éléments obligatoires d'un certificat sont :</p> <ul style="list-style-type: none"> - la clé publique de l'émetteur (identifiant de l'émetteur de certificat), - la clé publique du « sujet » (identifiant du détenteur de la clé privée associée à cette clé publique), - le type de certificat, - la version de certificat, - l'adresse où est décrit le type de certificat, sa structure et sa sémantique: <i>profileURL</i>, - les adresses où obtenir d'autres certificats sur l'émetteur du présent certificat (<i>issuerCertRepository</i>), - les adresses où obtenir d'autres certificats sur le « sujet » du présent certificat (<i>subjectCertRepository</i>). <p>On voit que le certificat contient des adresses de serveurs pouvant fournir d'autres certificats permettant des échanges automatiques en réseau entre diverses parties de façon à obtenir un système plus sophistiqué d'établissement de la confiance, d'affermissement des conditions de la fiabilité, et de raffinement dans le contrôle des autorisations grâce aux</p>

	<p>schémas des entités de <i>groupe</i> et des modèles de <i>rôle</i>. Ces intermédiaires de représentation sont présentés comme un moyen de certification mieux adapté aux exigences des parties ne se connaissant pas au préalable pour se faire confiance lors d'échanges et de transactions en réseau ouvert.</p> <p>TPL est un langage pour définir des groupes ainsi que les règles qui déterminent comment on peut en devenir membre. Une structure TPL a pour racine une politique, laquelle peut comprendre plusieurs groupes. Les membres d'un groupe sont représentés par leur clé publique de sorte qu'on peut faire correspondre un groupe à un <i>rôle</i> sur le plan du contrôle d'accès. Un groupe a un attribut <i>nom</i> et il contient une règle : une règle est une fonction appliquée aux valeurs dans les champs d'un certificat de clé publique pour déterminer si une personne est membre ou si elle peut le devenir. Une règle spécifie une fonction à évaluer dans le certificat. Cette fonction s'alimente aux deux autres éléments contenus dans une règle : l'inclusion et l'exclusion permettent de définir des filtres sur les valeurs présentes dans les certificats. La fonction d'une règle peut être une arborescence complexe avec des opérateurs logiques et des éléments champs (ceux du certificat) et un élément constante pour établir une valeur de référence fixe.</p>
--	---

Remarque

Lexique anglais-français

Rédacteur : Richard Parent
Organisation source : Secrétariat du Conseil du trésor
Date de publication : 10 novembre 2000
Raison d'être : Connaissance technologique
Programme gouvernemental : Inforoutes et ressources informationnelles
Nom du modificateur :
Date de dernière modification :
Note numéro : 73