

Statut du document	<i>Committee Working Draft</i>
Titre	<i>XACML Language Proposal, version 0.8</i> (XACML : XML Access Control Markup Language) Langage de balisage du contrôle d'accès
Mot clé	Attestation et sécurité
Source	OASIS www.oasis-open.org/committees/xacml/docs/docs.shtml
Date de publication	10 janvier 2002
Nombre de pages	37
Langue	Anglais
Lien avec autres normes	Fonctionnement en tandem prévu des politiques de contrôle d'accès en XACML avec les énoncés et messages en SAML
Situation actuelle	
Description	<p>XACML est un langage pour les politiques de contrôle d'accès : on veut permettre l'application de contraintes multiples. Trois modèles servent à comprendre le fonctionnement de XACML : la circulation des données, le langage de politique, l'administration.</p> <p>Modèle 1 : Circulation des données selon les étapes générales suivantes :</p> <ol style="list-style-type: none"> 1- Un ou des Points d'administration alimentent un Centre de rassemblement de politique qui doit s'assurer de rassembler toutes les règles faisant partie de la politique applicable; en cas de conflit de politique, il demande l'intervention d'un Centre de médiation de politique pour obtenir comme résultat une politique applicable cohérente. 2- Le Seuil d'application de politique envoie une demande de décision au Centre de décision de politique sous forme d'une requête d'autorisation SAML. Cette requête de décision comprend un, quelques-uns ou tous les attributs requis par le Centre de décision pour prendre une décision, en conformité avec la politique. 3- Le Centre de décision formule une demande d'instance de politique applicable au Centre de rassemblement de politique. La formulation dépend de la classification de la ressource et de l'action concernée. 4- Le Centre de rassemblement de politique répond au Centre de décision avec la politique applicable complète sous forme d'une instance XACML. 5- Le Centre de décision de politique examine la demande de décision qu'il avait envoyée ainsi que la politique applicable obtenue pour vérifier qu'il y a toutes les valeurs d'attribut requises pour que soit rendue une décision d'autorisation. Si ce n'est pas le cas, il envoie des demandes d'attributs SAML à des Sources d'information de politique pertinentes. 6- La Source d'information (possiblement une Autorité d'attribut SAML) peut éventuellement s'adresser à des sources externes aux rôles prévus par XACML, et il doit retourner au Centre de décision des réponses contenant des énoncés SAML d'attribut. 7- Le Centre de décision évalue l'instance de politique et effectue les post-conditions internes s'il s'en trouve dans cette politique. 8- Si la politique est évaluée comme VRAI, une fois que les post-conditions internes ont été exécutées, le Centre de décision retourne une décision d'autorisation sous forme de réponse SAML d'autorisation au Seuil d'application; cette réponse contient la décision « permettre » pour un attribut et toute post-condition externe. <p>Modèle 2 : Langage de politique qui comprend six parties :</p> <ol style="list-style-type: none"> 1- Attributs de titre et de rôle : une demande d'attribut se fait à propos d'un seul

titre. Les instances de politique XACML peuvent référer aux attributs d'un titre particulier ou à un rôle assigné à ce titre. Ce sont les énoncés SAML d'attribut qui servent au Centre de décision de politique pour confirmer qu'un titre occupe un rôle spécifié dans la politique. Des attributs peuvent être associés soit à des titres soit à des rôles par diverses Autorités d'attribut. La vérification des sources d'autorité relève de la responsabilité du Centre de décision.

- 2- Attributs de ressource et de classification : une demande d'autorisation a trait à une seule ressource. Les instances de politique XACML peuvent référer aux attributs d'une ressource particulière ou à une classification de la ressource. C'est le Centre de décision qui est responsable de vérifier que la ressource occupe la classification exigée et de résoudre les références d'attribut de la politique XACML, ainsi que les sources d'énoncés d'attribut. Si la ressource est un document XML, la classification de la ressource peut être un attribut ou un élément de la ressource elle-même. Dans d'autres cas, ce peut être des énoncés SAML provenant d'autorités d'attributs.
- 3- Attributs d'environnement : les instances de politique XACML peuvent référer à des attributs qui ne sont pas directement associés avec un titre ni avec une ressource. On les appelle des attributs d'environnement, par exemple la date et l'heure. Les attributs d'environnement sont distribués comme des énoncés SAML provenant d'autorités appropriées (responsabilité de vérification par le Centre de décision).
- 4- Classification, action, ressource et cible : les instances de politique sont associées à des paires classification-action. Le Centre de décision s'en sert pour vérifier que l'action identifiée dans la demande d'autorisation est bien celle qui se trouve dans l'instance de politique, et que la ressource identifiée appartient bel et bien à la classification identifiée dans l'instance de politique. L'algorithme pour apparier un nom de ressource à un nom de classification est identifié par un URI.
- 5- Politique, règle, pré-condition, prédicat : les instances de politique XACML sont bâties par la combinaison de règles. Chaque règle comporte une pré-condition et une ou plusieurs post-conditions. Une pré-condition est un opérateur logique ou un prédicat. Un prédicat est un énoncé à propos d'attributs qui peuvent être vérifiés par le Centre de décision de politique. Si l'instance de politique applicable à une demande d'autorisation évalue à VRAI, et si toutes les post-conditions internes ont été satisfaites, alors le Centre de décision peut retourner une décision d'autorisation d'attribut avec la valeur « permettre » au Seuil d'application de politique.
- 6- Post-condition : les post-conditions sont les actions spécifiées dans l'instance de politique XACML. Les post-conditions sont de deux types, les internes qui doivent être satisfaites avant l'émission d'une décision d'autorisation avec la valeur « permettre », et les externes que le Centre de décision transmet au Seuil d'application de politique.
- 7- Identification d'attribut : Le nom de l'autorité source et le nom du type de l'attribut forment ensemble l'identification de l'attribut. Le Centre de décision doit vérifier que la demande identifie une autorité reconnue dans une liste de référence.

Modèle 3 : **Administration**

Il est essentiel que les instances de politique XACML ne contiennent de référence qu'à des attributs et des post-conditions qui sont accessibles au Centre de décision et au Seuil d'application. Ceci oblige à ce que chaque autorité d'attribut SAML fournisse une interface grâce à laquelle les Points d'administration de politique peuvent découvrir les types d'attribut qui y sont accessibles.

	<p>Syntaxe de politique</p> <ul style="list-style-type: none"> - <i>Politique applicable</i> : élément de niveau supérieur, il contient un élément <i>cible</i> qui indique les ressources auxquelles une politique s'applique) et un élément <i>politique</i> qui contient la politique elle-même. - <i>Type de cible</i> : élément qui contient une description des cibles sous forme d'éléments de « classification de ressource » et de « SAML:Actions ». Le Centre de décision doit se baser sur la cible pour sélectionner la bonne instance de politique et traiter une demande SAML d'autorisation : ce qui est demandé doit être inclus dans ce qui est permis. - <i>Type de politique</i> : élément qui regroupe des règles et les interrelie par des opérations logiques, et les accompagne facultativement de post-conditions. - <i>Signature</i> : élément conforme à XML Dsig. - <i>Type de règle</i> : élément dérivé de type de règle abstrait en restreignant le nombre d'éléments à seulement un des choix, de manière que les prédicats soient reliés par des opérateurs logiques et non simplement listés : type ET, type OU, type PAS. - <i>Type de règle abstrait</i> : élément qui contient soit un opérateur logique soit un prédicat. - Prédicat : comparaison avec égal, plus grand ou égal, plus petit ou égal, sous-ensemble de, sur-ensemble de, forme appariée, ensemble non nul d'intersection; outre une comparaison, le prédicat peut référer à une fonction externe (une définition WSDL). <p>Quelques autres définitions complètent cette syntaxe.</p> <p>Il est prévu de décrire des profils de XACML pour des classes générales de problèmes, de décrire le sous-ensemble de SAML pertinent, un profil de XML Dsig, et un schéma LDAP pour les cas où LDAP sera utilisé pour distribuer XACML.</p>
--	---

Remarque Le texte contient encore beaucoup de questions ouvertes, de nombreuses précisions restent à apporter.

Lexique anglais-français

Access control	Contrôle d'accès	Exercice du contrôle d'accès en accord avec une politique applicable
Access	Accès	Pouvoir exercer une action sur une ressource Note : accès ne se limite pas ici au franchissement d'un seuil, il porte aussi sur les actions possibles effectuées sur les ressources accédées
Applicable policy	Politique applicable	L'ensemble complet des règles qui déterminent l'accès à une ressource spécifique.
Action	Action	Opération qui peut être effectuée sur la ressource
Attribute	Attribut	Caractéristique d'un titre, d'une ressource ou d'un environnement qui peut être référencée par une pré-condition Dans le vocabulaire XACML, le terme attribut est utilisé à la place de termes jugés équivalents comme

		privilège, permission, droit, autorisation, et habilitation.
Attribute specifiers	Déterminants d'attribut	Nom d'autorité source et nom du type de l'attribut forment l'ensemble constituant l'identification de l'attribut.
Authorization decision	Décision d'autorisation	Le résultat de l'application de la politique applicable. Il s'agit d'une fonction de portée booléenne et, facultativement, un ensemble de post-conditions
Classification	Classification	Un ensemble d'attributs pertinents à une ressource
Context	Contexte	L'usage voulu d'une information tel que révélé comme un résultat de l'accès
Decision request	Demande de décision	La demande adressée par un seuil d'application de politique à un centre de décision de politique
Environment	Environnement	L'ensemble des attributs qui peuvent être référencés par des pré-conditions et qui sont indépendantes d'un titre et d'une ressource en particulier
Information request	Demande d'information	La demande adressée par un centre de décision politique à une source d'information de politique pour un ou plusieurs attributs d'environnement
Pattern match	Forme appariée	Résultat de comparaison
Permit	Permettre	Valeur de décision pour un attribut dans une réponse d'autorisation
Policy administration point (PAP)	Point d'administration de politique	Entité de système qui crée la politique applicable. Note : pour le mot anglais <i>point</i> , l'équivalent français « point » respecte l'idée de dispersion des sources
Policy conflict	Conflit de politique	L'état qui existe quand deux ou plusieurs pré-conditions faisant partie de la politique applicable, conduisent chacune à des résultats interférant l'un avec l'autre
Policy decision point (PDP)	Centre de décision de politique	Entité de système qui évalue la politique applicable. Note : pour le mot anglais <i>point</i> , l'équivalent français « centre » traduit l'aspect sommatif, portant sur l'information complète de la décision
Policy enforcement point (PEP)	Seuil d'application de politique	Entité de système qui effectue le contrôle d'accès, en permettant ou non les opérations selon la politique applicable. Note : pour le mot anglais <i>point</i> , l'équivalent français « seuil » traduit l'idée que le franchissement peut être permis ou empêché
Policy information point (PIP)	Source d'information de politique	Entité de système qui agit comme lieu d'obtention d'information sur les attributs d'environnement. Note : pour le mot anglais <i>point</i> , l'équivalent français « source » caractérise le rôle de bibliothèque de référence de cette entité
Policy mediation point (PMP)	Centre de médiation politique	Entité de système qui résout les conflits de politique. Note : pour le mot anglais <i>point</i> , l'équivalent français « centre » traduit le caractère nécessairement intégrateur d'un arbitrage entre énoncés contradictoires

Policy retrieval point (PRP)	Centre de rassemblement de politique	Entité de système qui garantit que la politique applicable est complète Note : pour le mot anglais <i>point</i> , l'équivalent français « centre » traduit le caractère nécessairement sommatif et intégrateur du caractère complet à assurer
Post-condition	Post-condition	Un processus spécifié dans une règle qui doit être complété en conjonction avec l'accès. Il y a deux types de post-condition : soit qu'une post-condition interne doive être exécutée par le centre de décision de politique avant d'émettre sa réponse « permettre », soit qu'une post-condition externe doive être exécutée par le seuil d'application de politique avant de permettre l'accès.
Predicate	Prédicat	Énoncé à propos d'attributs dont on peut évaluer la valeur en termes de vrai ou faux
Pre-condition	Pré-condition	Un prédicat ou un ensemble logiquement combiné de prédicats
Principal	Titre	Une entité de système pouvant être référencée par une pré-condition. Un titre rattache une entité à une clé cryptographique (son secret), capable de générer une signature numérique. Équivalent de « sujet » ou d'un utilisateur. Note terminologique : en droit, un titre est un acte écrit, une pièce authentique qui sert à établir un droit, une qualité.
Resource	Ressource	Composant de données, de service ou de système. Terme équivalent à Objet tel que souvent utilisé.
Role	Rôle	Un ensemble d'attributs pertinents à un titre. En XACML, un « groupe » est traité comme s'il était un rôle parce qu'il n'y a pas de différence du point de vue de la décision d'accès.
Rule	Règle	La combinaison d'une pré-condition ainsi que d'une ou plusieurs post-conditions
Target	Cible	L'ensemble des ressources et actions auxquelles une politique applicable s'applique

Rédacteur : Richard Parent
Organisation source : Secrétariat du Conseil du trésor
Date de publication : 27 mars 2002
Raison d'être : Connaissance technologique
Programme gouvernemental : Inforoutes et ressources informationnelles
Nom du modificateur :
Date de dernière modification :
Note numéro : 121