

| | |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Statut du document | <i>Committee Working Draft</i> |
| Titre | <i>Security Assertions Markup Language (SAML)</i> Langage de balisage des déclarations de sécurité |
| Mot clé | Attestation et sécurité |
| Source | OASIS http://www.oasis-open.org/committees/security/ |
| Date de publication | 10 janvier 2002 |
| Nombre de pages | 53 |
| Langue | Anglais |
| Lien avec autres normes | Basé en bonne partie sur les concepts élaborés dans AuthML et S2ML qui se sont joints au travail sur SAML. |
| Situation actuelle | Le transport de SAML a été défini pour SOAP sur HTTP |
| Description | <p>L'idée générale de SAML est de permettre une déclaration unifiée des autorisations sous une gestion centralisée. Ce document décrit la syntaxe et la sémantique pour encoder en XML des déclarations SAML et un protocole de demandes et de réponses. L'information de sécurité se compose d'énoncés à propos de sujets. Ces déclarations sont émises par des autorités SAML : autorités d'authentification, autorités d'attribut, centres de décision de politique. Le protocole SAML permet aux clients d'interroger ces autorités.</p> <p>Il y a trois types d'énoncés qui peuvent être déclarés, soit des énoncés :</p> <ul style="list-style-type: none"> - d'Authentification : le sujet désigné a été authentifié par un moyen particulier à un moment particulier - d'Attribut : le sujet désigné est associé aux attributs fournis. - de Décision d'autorisation : une demande pour laisser le sujet désigné accéder à la ressource spécifiée a été accordée ou refusée <p>En SAML, deux types simples interviennent dans les déclarations :</p> <ul style="list-style-type: none"> - <i>IDType</i> pour déclarer et référencer les identifiants de déclarations, de demandes et de réponses - <i>DecisionType</i> pour définir les valeurs pouvant être rapportées comme statut d'un énoncé de décision d'autorisation. <p>Les Déclarations SAML peuvent contenir les éléments suivants :</p> <ul style="list-style-type: none"> - <i>AssertionSpecifier</i> : élément qui indique comment est faite la déclaration : soit par référence à une déclaration SAML (<i>AssertionID</i>), soit en donnant la valeur de l'attribut (<i>Assertion</i>) |

- L'élément *Assertion* (déclaration) contient obligatoirement des indications de version SAML, un identifiant de déclaration, le nom ou l'URI de son émetteur, le moment horodaté de son émission, ainsi que, facultativement, des conditions de validité de la déclaration et un avis pouvant être utilisé pour le traitement; enfin et surtout, cet élément contient un ou plusieurs énoncés : énoncé de sujet, énoncé d'authentification, énoncé de décision d'autorisation, énoncé d'attribut.

- L'élément *Conditions* qui peut être contenu dans une déclaration doit être entièrement validé pour que la déclaration puisse être tenue pour valide. Les conditions peuvent être exprimées en termes de *Pas avant* et *Pas pendant ou après* qui permettent de délimiter un intervalle de validité; en termes de *restriction d'auditoire* par un URI contenant une liste ou description; en termes de *restriction à une partie ciblée* (URI aussi) pour la déclaration.

Les énoncés SAML sont composés des principaux éléments suivants :

- un élément *Sujet* peut contenir un ou plusieurs sujets, avec leur *Nom* et celui de leur *Domaine de sécurité*, chaque sujet n'ayant qu'un titre pour le sous-élément *Confirmation de sujet*, lequel se décompose à son tour en un URI identifiant un protocole comme *Méthode de confirmation*, et les données de la valeur pour l'authentification (signature XML ou autre).

- un élément *Énoncé d'authentification* qui précise selon quelle *Méthode d'authentification* et à quel moment (*AuthenticationInstant*), et facultativement à quelle localisation (nom de domaine - DNS - et adresse - IP).

- un élément *Lien d'autorité* peut spécifier la *Sorte d'autorité* (authentification, attribut, autorisation) et l'adresse de cette autorité.

- un élément *Énoncé de décision d'autorisation* est ce qui est transmis par un Centre de décision de politique à un Seuil d'application de politique. Il réfère à un Sujet par rapport à l'accès à une Ressource (URI) et il indique une *Décision* (permettre) relative à des Actions. Il peut aussi faire état de l'*Évidence* sur laquelle la décision a été appuyée.

- un élément *Énoncé d'attribut* associe un Attribut à un Sujet. L'attribut est indiqué par une *Désignation d'attribut* avec un *Nom d'attribut* dans un *Espace nominatif d'attribut*, et la *Valeur d'attribut*.

Le **Protocole SAML** est un moyen supplémentaire aux implantations de SAML par rattachement aux protocoles en usage. Le Protocole

SAML définit deux éléments, la Demande transmise par un client et la Réponse fournie par un service SAML. Les **Demandes** SAML comportent obligatoirement un identifiant de demande, un indicateur de version SAML, et un ou des « Répondre par ». L'élément Répondre par sert à indiquer un type de réponse acceptable pour le demandeur au moyen de l'une des valeurs suivantes :

- Énoncé unique : la déclaration ne contient qu'un seul énoncé
- Énoncé multiple : la déclaration contient au moins un énoncé
- Énoncé d'authentification
- Énoncé de décision d'autorisation
- Énoncé d'attribut
- URI de schéma

Une demande SAML peut porter sur une déclaration spécifique ou contenir une requête d'authentification, d'attribut ou de décision d'autorisation.

Les **Réponses** SAML comportent obligatoirement un identifiant de réponse, une référence à l'identifiant de demande, un indicateur de version SAML et le contenu de la réponse qui assigne un statut à la demande SAML correspondante et une liste de zéro à plusieurs énoncés. Une liste de statuts est prédéfinie : Succès, ou indication soit de problème de version, ou d'erreur due au demandeur ou au service. Le statut peut être précisé au moyen d'un code de sous-statut précisant un message d'erreur dont quelques-uns sont définis : version de demande trop élevée ou trop basse, ou désuète, ou trop de réponses pour l'envoi à effectuer.

Le versionnage du protocole SAML est traité en détail, y compris les versions de déclaration, de demande, et de réponse.

Les messages SAML de déclaration, demande et réponse doivent être signés s'ils sont échangés hors d'un domaine de sécurité. La signature préférée est XML Sig. Une signature d'un ensemble peut s'appliquer par héritage à tout élément de cet ensemble : ainsi une déclaration SAML peut être incluse dans un document plus étendu qui est signé. Un profil du standard *XML Signature* est défini pour SAML :

- recours au type *enveloppé* de signature (pas le type *enveloppant*, ni le type *détaché*)
- régularisation de chaîne de caractères à signer selon standard *Canonical XML* sans commentaires
- recours à la transformation « xmldsig#enveloped-signature »
- KeyInfo : facultatif en SAML.

Une présentation est faite des manières de faire des extensions conformes en SAML et des règles à suivre.

| | |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | SAML définit un certain nombre d'identifiants qui le situent dans son contexte de déploiement technique. Ces identifiants sont des URI : - pour des protocoles servant de Méthode de confirmation : Artifact SAML, SHA-1, Kerberos, SSL/TLS, PKCS/7, XML-SIG, etc. - pour des identifiants d'action : URI pour les définitions courantes d'actions sur les ressources : Lire, Écrire, Exécuter, Supprimer, Contrôler (i.e. spécifier le contrôle d'accès), indication négative d'action par le tilde, actions HTTP (<i>get, head, put, post</i>), permissions Unix. |
| Remarque | |
| Lexique anglais-français | |

| | | |
|----------------------------------|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | | |
| Assertion | Déclaration | Paquet d'information contenant un ou plusieurs énoncés faits par un émetteur. Note : en droit, affirmation écrite faite par une partie ou un témoin et portant sur l'existence d'une situation juridique ou d'un fait. |
| AttributeNamespace | Espace nominatif d'attribut | |
| AttributeStatement | Énoncé d'attribut | |
| Authentication Statement | Énoncé d'authentification | |
| AuthorityBinding | Lien d'autorité | |
| Authorization Decision Statement | Énoncé de décision d'autorisation | |
| MultipleStatement | Énoncé multiple | |
| Query | Requête | |
| Request | Demande | |
| RespondWith | Répondre par | |
| Response | Réponse | |
| SingleStatement | Énoncé unique | |
| Statement | Énoncé | Chacune des associations au sujet pouvant être listées dans une déclaration est affirmée comme un fait, une chose vraie |