

Statut du document	<i>W3C Note</i>
Titre	<i>XML Key Management Specification (XKMS)</i> Définition en XML de la gestion de clés
Mot clé	Attestation et sécurité
Source	http://www.w3.org/TR/2001/NOTE-xkms-20010330/
Date de publication	30 mars 2001
Nombre de pages	68
Langue	Anglais
Lien avec autres normes	Intégration avec XML et normes de chiffrement et signature numériques du W3C/IETF, ainsi que les protocoles SOAP et WSDL.
Situation actuelle	Proposition publique de Verisign, Microsoft, webMethods, au W3C (<i>XML Activity on XML Protocols</i>) comme solution d'emballage de message. À l'origine, constituait une partie des <i>XML Trust Services</i> de Verisign.
Description	<p>La meilleure façon d'augmenter la sécurité des échanges par Internet semble aujourd'hui de combiner la précision permise par XML avec les meilleurs moyens connus de sécurité soit les certificats de clé publique. XML est le mécanisme général pour intégrer des applications réparties par l'Internet. XKMS s'inscrit dans cet axe en proposant un vocabulaire formel pour l'intégration, dans les applications permettant les transactions Internet, de la sécurité par le recours à des certificats de clé publique, à la signature numérique de documents et au chiffrement (encryptage) de l'information. C'est pour faciliter cette intégration que XKMS offre de contrôler les divers logiciels de gestion de certificats (Entrust, Baltimore...) au moyen de transactions XML, épargnant aux développeurs d'applications d'avoir à se mesurer à la complexité reconnue de tels logiciels. L'objectif est de déployer une <i>architecture XML de confiance</i> en combinant pour le mieux les dispositions relatives à la signature et au chiffrement des documents et de leurs éléments. Le recours à XML bénéficie aussi à la sûreté d'accès vis des interfaces réduites (cellulaire) en permettant de déplacer vers le serveur les principaux composants reliés à la confiance.</p> <p>La gestion de clés selon XKMS se subdivise en deux composants :</p> <ul style="list-style-type: none"> - X-KISS (<i>XML Key Information Service Specification</i>) définit un service d'échange (paires de requête-réponse) XML pour localiser ou valider l'<u>information</u> associée à une clé publique, ce qui rend possible un traitement non plus dans le poste client, mais dans un serveur. - X-KRSS (<i>XML Key Registration Service Specification</i>), définit un service en XML pour l'<u>enregistrement</u> d'une paire de clés (PGP, X.509v3 ou autre) par son détenteur en vue de la rendre utilisable en conjonction avec XKMS. Les paires de messages définies ont trait à l'enregistrement, à la révocation du certificat de clé publique, et à la récupération de la clé secrète lorsqu'elle avait été confiée.

Remarque

Lexique anglais-français

Rédacteur : Richard Parent
Organisation source : Secrétariat du Conseil du trésor
Date de publication : 12 décembre 2000
Raison d'être : Connaissance technologique
Programme gouvernemental : Inforoutes et ressources informationnelles
Nom du modificateur : Richard Parent
Date de dernière modification : 20 août 2001

Note numéro :

82