

Statut du document	<i>W3C Candidate Recommendation</i>
Titre	<i>XML Encryption Requirements</i> <i>XML Encryption Syntax and Processing</i> <i>Decryption Transform for XML Signature</i> Chiffrement XML : exigences, syntaxe et traitement, transformation de déchiffrement pour la signature numérique
Mot clé	Attestation et sécurité
Source	Exigences W3C : http://www.w3.org/TR/xml-encryption-req Syntaxe et traitement : http://www.w3.org/TR/xmlenc-core/ Transformation de déchiffrement : http://www.w3.org/TR/xmlenc-decrypt
Date de publication	4 mars 2002
Nombre de pages	Exigences : 10 Syntaxe et traitement : 45 Transformation de déchiffrement : 10
Langue	Anglais
Lien avec autres normes	Famille XML de normes, branche syntaxique de responsabilité effective du W3C. <i>XML Encryption</i> est un protocole dont l'utilité est la même que TLS ou SSL, mais qui permet toutefois de faire des choses plus sophistiquées, par exemple transporter des éléments confidentiels avec d'autres éléments qui ne le sont pas dans un contexte d'affaires. Utilise <i>XML Signature</i> .
Situation actuelle	
Description	<p>Le document principal, qui porte sur la syntaxe et le traitement, présente un processus pour chiffrer l'information et représenter le résultat en un élément XML. Un cryptogramme résulte du chiffrement. Le contenu (valeur), une fois rendu inintelligible, peut être placé dans l'élément <i>information chiffrée</i> directement, mais cette valeur peut aussi n'y être que référée. La valeur chiffrée est ce qui se substitue au texte en clair, mais qui ne devait pas être laissé en un état intelligible pour toute personne n'ayant pas d'abord obtenu une clé.</p> <p>Le chiffrement est applicable à un élément XML en entier y compris les balises; il peut aussi être appliqué sélectivement à certains des éléments d'un document, mais pas tous, ou même au contenu de la valeur d'un seul élément ou d'un seul attribut; le chiffrement peut tout autant être appliqué sans les balises; il peut aussi être appliqué à un paquet comprenant des éléments XML traités comme toute autre séquence de données. Tout fragment d'information peut se voir appliquer le chiffrement.</p> <p>Le cryptogramme peut inclure un élément <i>méthode de chiffrement</i> et l'<i>information de clé</i> en plus de l'information chiffrée. La méthode de chiffrement réfère à un algorithme et l'information de clé lui est associée. Des propriétés peuvent être associées au chiffrement et diverses modulations sont possibles selon les méthodes. En particulier, il faut fournir des indications sur l'ordre dans lequel les opérations de chiffrement et de signature ont été exécutées pour que les opérations inverses de déchiffrement et de vérification de signature puissent être correctement exécutées. C'est la transformation de déchiffrement qui règle cette étape.</p> <p>Ce protocole a un caractère très technique, avec des spécifications précises et détaillées. Une table des algorithmes et de leurs utilisations possibles est incluse dans le protocole dans sa partie 5 afin de faciliter l'interopérabilité des implantations hétérogènes.</p>

Remarque

Lexique anglais-français

Ciphered data	Information chiffrée	Élément du cryptogramme contenant soit la valeur chiffrée elle-même, soit une référence à la localisation de cette valeur chiffrée.
Cipher reference	Référence à la valeur chiffrée	Dans l'élément <i>information chiffrée</i> , remplacement de la valeur de l'information chiffrée par une référence à la localisation de cette valeur.
Cipher value	Valeur chiffrée	La suite de caractères illisibles résultant du chiffrement et qui prend la place du contenu informationnel dans l'élément <i>information chiffrée</i> .
Decryption	Déchiffrement	Opération inverse d'un chiffrement réversible, permettant à une personne autorisée, en possession de la clé, de rétablir en clair un cryptogramme.
Decryption Transform	Transformation de déchiffrement	
Encrypted Data	Cryptogramme	Contenu rendu inintelligible grâce au chiffrement, qui ne peut être compris et utilisé que par les seules personnes en possession de la clé qui permet de le déchiffrer.
Encryption	Chiffrement	Opération par laquelle est substitué, à un texte en clair, un texte inintelligible, inexploitable pour quiconque ne possède pas la clé permettant de le ramener à sa forme initiale. Note : <i>Cryptage</i> est un synonyme de <i>chiffrement</i> , mais <i>décryptage</i> n'est pas synonyme de <i>déchiffrement</i> , puisqu'il désigne le déchiffrement par cryptanalyse, qui consiste à traduire en clair un cryptogramme dont on ne possède pas la clé.
Key Info	Information de clé	

Rédacteur : Richard Parent
Organisation source : Secrétariat du Conseil du trésor
Date de publication : 10 juillet 2002
Raison d'être : Connaissance technologique
Programme gouvernemental : Inforoutes et ressources informationnelles
Nom du modificateur :
Date de dernière modification :
Note numéro : 128