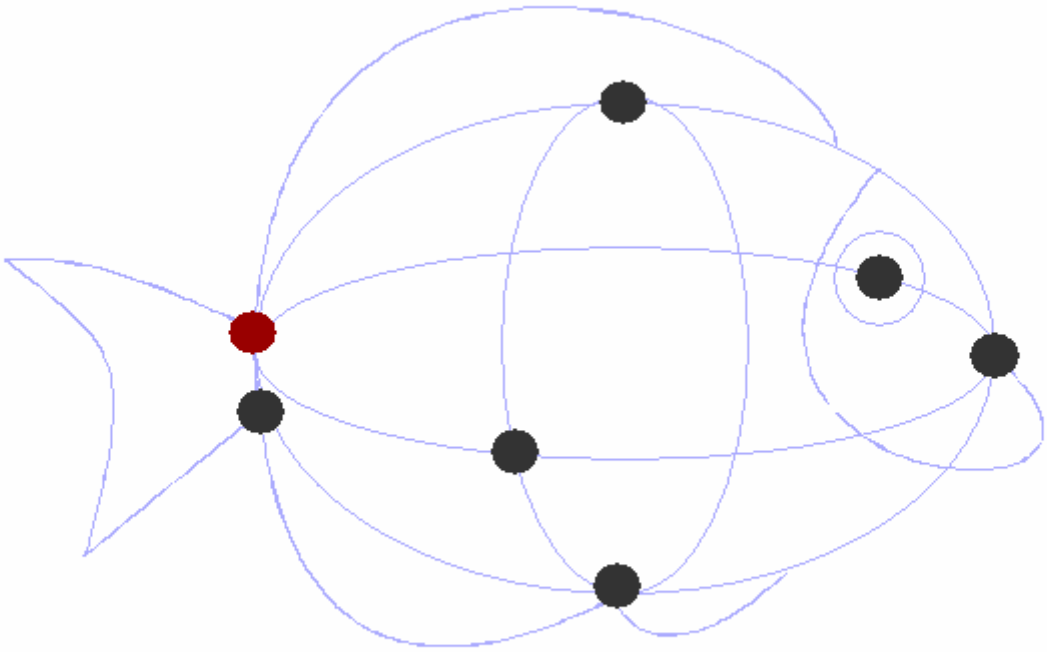
Référence du document :	WLSign.AUD.0001
Révision du document :	1.3
Date du document :	15/03/2011

Worldline Signer Server

Cible de sécurité



www.atosworldline.com

Table des matières

Table des figures

Historique des révisions de document

Version	Date	Auteur	Motif
1.0	09/09/2010	Atos Worldline	Première version publique
1.1	27/10/2010	Atos Worldline	Prise en compte premiers retours auditeur
1.2	15/02/2011	Atos Worldline	Prise en compte rapport de pré-évaluation
1.3	15/03/2011	Atos Worldline	Corrections

Références

Version	Motif
[CRYPTO-1]	Mécanismes cryptographiques - Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques Vers.1.20
[CRYPTO-2]	Gestion de clés - Règles et recommandations concernant la gestion des clés utilisées dans les mécanismes cryptographiques. Vers.1.10
[RGS-A10]	Politique de certification «Cachet» Version 2.3 du 11 février 2010
[RGS-A5]	Fonction de sécurité «Cachet» Version 2.3 du 11 février 2010
[PKCS#11]	PKCS #11: Cryptographic Token Interface Standard Version 2.30

1 IDENTIFICATION

Eléments	Valeur
Titre	**Worldline Signer Server Cible de Sécurité**
Référence document	**WLSign.AUD.0001**
Version cible	**1.3**
Auteur	**Atos Worldline**
Référence produit	**Worldline Signer Server**
Version produit	**1.0**
Catégorie du produit	**identification, authentification et contrôle d'accès**
Mots clé	**Signature électronique, Application de signature électronique, Application de création de signature électronique, Application de validation de signature électronique, validation de signature électronique**

2 ARGUMENTAIRE DU PRODUIT

2.1 DESCRIPTION GENERALE DU PRODUIT

Le produit Worldline Signer Server est package permettant de réaliser les services,

- D'une application de cachet serveur
- D'un module de vérification de cachet serveur,

Il est ainsi possible de réaliser les opérations de création et de vérification de cachet serveur pour une application appelante (service applicatif).

Le produit se décompose en deux parties distinctes :

- une interface Java générique offrant les méthodes de base (création et fermeture de service, signature, vérification),
- un système de paramétrage (statique ou dynamique) regroupant toute la description du service qui sera implémenté par le produit.

Le produit n'est pas destiné à une utilisation directe par un humain, il n'y a pas d'IHM.

2.1.1 Schéma logique du produit

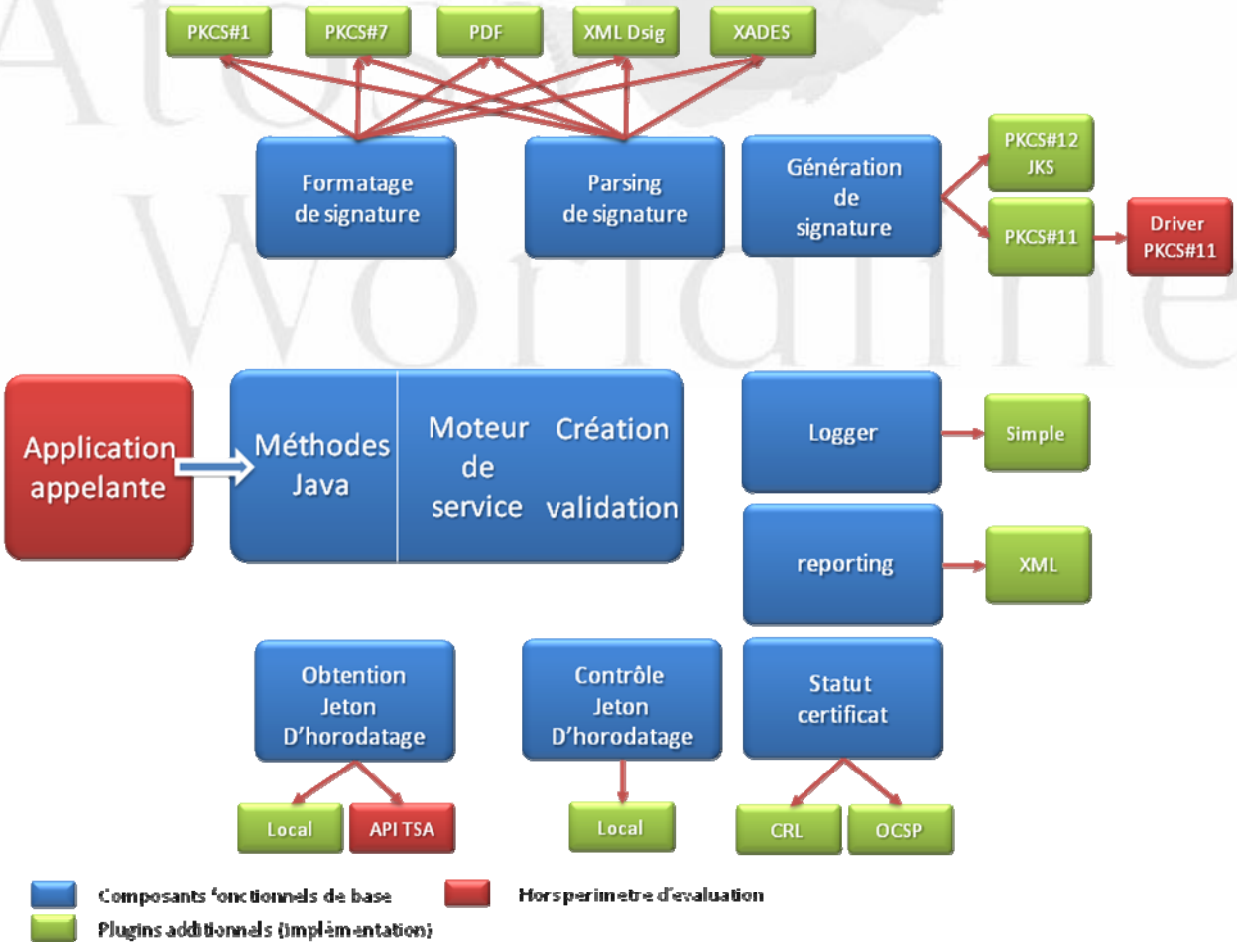


Figure 1 : schéma logique fonctionnel

2.2 DESCRIPTION DE LA MANIERE D'UTILISER LE PRODUIT

Le produit est invoqué uniquement par une application cliente en mode « programmatique » par appel de méthodes java correspondantes aux services rendus.

L'utilisation courante du produit peut se décrire en plusieurs étapes successives :

- chargement des paramètres,
- création du service correspondant aux paramètres chargés,
- appel des services de création de signature ou validation de signature,
- fermeture du service.

2.3 DESCRIPTION DE L'ENVIRONNEMENT PREVU D'UTILISATION DU PRODUIT

Le produit est constitué de librairies Java afin de pouvoir fonctionner sur n'importe quelle plateforme (OS / matériel) supportant une JVM.

Le produit est destiné à être utilisé exclusivement en interne des applicatifs Atos Worldline sur ses propres moyens de production ou dans le cadre de projet où Atos Worldline fournit le support à la mise en œuvre et à l'exploitation

De ce fait le produit Worldline Signer Server, ainsi que les matériels utilisées sont administrés et pilotés uniquement par du personnel habilité tant du point de vue des exploitants que des développeurs.

L'environnement ainsi mis en œuvre pour héberger le produit, sur les serveurs doit répondre aux exigences, en termes d'environnement d'utilisation, tels que décrit dans le document **[RGS-A5]**

Optionnellement, il pourra interroger des composants distants par une requête réseau, vers des serveurs externes hors du périmètre de l'évaluation (horodatage, OCSP, CRL).

Le produit est capable d'utiliser un support matériel (HSM) compatible avec le standard **[PKCS#11]** pour

- Le stockage des clés de signature
- La création de signature.

Le cycle de vie des clés n'est pas sous la responsabilité du produit. Les aspects initialisation, injection, renouvellement des clés, doivent être pris en charge par les développeurs des applications.

2.4 DESCRIPTION DES HYPOTHESES SUR L'ENVIRONNEMENT

2.4.1 Initialisation / Utilisation

Le guide d'installation recommande que l'environnement respecte certaines exigences de sécurité pour l'utilisation du produit.

Une bonne pratique au niveau des acteurs identifiés, consiste à se référer à une politique de sécurité interne à l'organisation qui utilise le produit et qui reprendrait notamment les points suivants :

- Protection contre les virus, politique de mise à jour permanente, surveillance permanente et, analyse régulière, information auprès des utilisateurs.

- Contrôle et limitations des échanges entre la machine hôte du produit et d'autres machines dans un réseau ouvert : habilitation de personnel pour administrer les équipements réseau via un workflow établi, surveillance dynamique des équipements réseau, cloisonnement des réseaux, identification et authentification de tous les accès et flux avec les réseaux publics.

- Restrictions d'accès aux fonctions d'administration par des administrateurs habilités : habilitation de personnel pour administrer les systèmes via un workflow établi, distinction compte administrateur et compte applicatif, traçabilité des actions, revue de compte, politique de changement périodique de mot de passe, Surveillance des accès.

- Installation et mise à jour de logiciel ou composants sous contrôle de l'administrateur : séparation des rôles, traçabilité, règles applicables par rôles. Workflow établi et contrôlé des affectations de rôles.

- Refus par le système d'exploitation de l'ordinateur d'exécuter des applications téléchargées ne provenant pas de sources sures : correspondance pour chaque applicatif d'un propriétaire désigné, procédure formelle et unique de chargement de code.

- Mise à jour de composants logiciels et systèmes lors de la mise à jour de sécurité : collecte des informations d'alertes de sécurité et conseils correspondants, mise en œuvre correctifs ou palliatifs par les équipes technique, traçabilité.

Il est recommandé également de prévoir des éléments de sécurité physique

  - Mettant en œuvre de règles de contrôle d'accès physique aux serveurs utilisant le produit
  - Assurant l'intégrité et la disponibilité des infrastructures ou sont positionnés les serveurs utilisant le produit

2.4.2 Personnel

Les personnels responsables de la fourniture et de l'exploitation des plateformes accueillant le produit sont considérés non hostiles. L'accès à ces plateformes tant du point de vue physique que réseau est contrôlé, et permet l'accès uniquement au personnel habilité

Le personnel est informé et accepte formellement ses responsabilité liées à la sécurité et reçoit régulièrement des informations de sensibilisation à la sécurité.

2.4.3 Configuration

La plateforme technique mise en place pour exploiter le produit est correctement administrée, par le personnel habilité

2.4.4 Horodatage

Le serveur sur lequel s'exécute le produit est à l'heure, pour cela une synchronisation NTP sur une base de temps (directe ou indirecte) est requise.

Le produit ne contrôle pas la conformité des jetons d'horodatage du point de vue du document **[RGA-A12],** toutefois

- les jetons utilisés par le produit sont conformes au standard RFC3161.
- Le certificat de signature du jeton d'horodatage possède l'extension « extended key usage » avec pour valeur l'OID=1.3.6.1.5.5.7.3.8 (timestamp)

2.4.5 Pilotage

Les alertes qui peuvent être remontées par le produit sont traitées par le personnel d'exploitation dans les meilleurs délais, et sont corrigées pour les alertes impactant le niveau de service.

La description du rôle et des droits du personnel d'exploitation est donné au chapitre *2.6.3 Exploitant*

2.4.6 Autorité de certification

Il est considéré pour l'évaluation que la PKI utilisée pour générer et gérer le cycle de vie des certificats utilisés par le service est fiable. C'est-à-dire

- Qu'elle met en œuvre des procédures suffisante pour assurer la fourniture de certificat dans de bonnes conditions de contrôle et traçabilité
- qu'elle ne permet pas de divulguer ou de rendre possible la divulgation des clés privées qu'elle gère.
- Qu'elle atteint un niveau de disponibilité satisfaisant, en particulier n'empêchant pas le fonctionnement nominal d'un outil de création ou validation de cachet serveur, notamment pour l'obtention de liste de révocation ou de réponse à une demande de statut de certificat de type OCSP

Le produit ne contrôle pas la conformité d'un certificat de cachet serveur, par rapport au document **[RGS-A10] et [RGA-A14].**
Toutefois le produit vérifie que

- le certificat possède l'extension « Key Usage » avec pour seule valeur : « digital signature ».
- que la taille de la clé est au minimum de 2048 bits
- que la durée du certificat n'excède pas 3 ans.

2.4.7 Cryptographie

Les clefs utilisées par le produit pour la création de signature sont conformes aux référentiels cryptographiques de l'ANSSI **[CRYPTO-1] [CRYPTO-2]** (longueur de clés, algorithme de hachage).

2.5 DESCRIPTION DES DEPENDANCES

Ces dépendances peuvent intervenir par rapport à des matériels, des logiciels et/ou des microprogrammes du système, et qui ne sont pas fournis avec le produit.

2.5.1 Librairie et support HSM

Lorsque l'application appelante choisit d'utiliser un support matériel pour le stockage et l'utilisation de clés privées (Hardware Secure Module), elle devra choisir un périphérique conforme avec le standard d'interfaçage **[PKCS#11].**

Le produit devra utiliser une librairie propriétaire PKCS#11 associée, livrée ou préconisée par le fournisseur du matériel HSM.

Cette librairie sera paramétrée par l'application appelante (nom, emplacement).

L'interface avec une librairie PKCS#11 fait partie de la cible d'évaluation.

La librairie PKCS#11 (driver) associée au support HSM ne fait pas partie du périmètre de la cible d'évaluation.

2.6 DESCRIPTION DES UTILISATEURS TYPIQUES

Ce paragraphe indique quels sont les acteurs concernés par l'utilisation et ou la mise en œuvre du produit.

2.6.1 Administrateur

L'administrateur est en charge de la mise à disposition et de la maintenance du ou des serveurs hébergeant le produit, il n'a pas de responsabilité opérationnelle directe sur l'utilisation directe du produit lui-même.

Droits : de part ses droits privilégiés, l'administrateur a un accès complet sur les serveurs.

2.6.2 Intégrateur

Ce sont les personnes qui sont chargés de l'installation du produit sur la machine ainsi que de son paramétrage avec les fichiers associés (keystore, certificat, crl, etc...).
L'intégrateur utilise un compte applicatif spécifique et dédié à l'application appelante sous lequel le produit de cachet serveur sera utilisé.
L'intégrateur a la responsabilité de se conformer aux indications du guide d'installation du produit.

Droits : lorsqu'il est habilité sur une application appelante, il peut utiliser le compte applicatif et ainsi dispose des droits en écriture et lecture pour l'ensemble du produit

2.6.3 Exploitant

Ce sont les personnes qui pilotent les serveurs supportant le produit. Ils reçoivent les alertes générées par le produit, et répercutent celle-ci vers les intégrateurs pour analyse.

Droits : Ils ne disposent pas d'accès en écriture sur l'ensemble du produit, ni d'accès en lecture sur les zones confidentielles

2.6.4 Application appelante

Il s'agit d'un logiciel local qui utilise les services du produit. L'application appelante s'exécute sous un compte applicatif spécifique et dédié.

Droits : Elle doit disposer uniquement des droits en lecture sur les répertoires de l'application appelante, et des droits en écriture sur le répertoire contenant les traces applicatives.

Note d'application 1 :

En fonctionnement, le produit n'est pas sollicité directement par un utilisateur humain, il n'y a donc aucune Interface Homme/Machine dans le produit.

Note d'application 2 :

Aucun autre acteur humain qui ne serait pas identifié ci-dessus, n'a légitimement accès au produit, sur une plateforme opérationnelle produisant des cachets serveur.

2.7 DEFINITION DU PERIMETRE DE L'EVALUATION

La cible d'évaluation est constituée de l'ensemble des éléments techniques logiciels et matériels qui contribuent à fournir le service de création et validation de signature électronique.

Le schéma (cf 2.1.1 Schéma logique du produit) permet de d'identifier ce périmètre :

- Composants fonctionnels de base : moteur du produit
- Plugins additionnels implémentant les différents services du produit.

3 ENVIRONNEMENT TECHNIQUE DE FONCTIONNEMENT

3.1 Matériel / OS

Le produit est compatible avec toute plateforme supportant une JRE conforme aux spécifications SUN J2SE 5 et supérieur.

Il n'existe pas de contraintes supplémentaires en termes d'Operating System.

3.2 Mesure d'environnement

Les recommandations en matière d'environnement d'exécution (cf. chapitre 2.4.1 de ce document) sont notées dans le guide utilisateur.

4 BIENS SENSIBLES A PROTEGER

4.1 Clef privée

Ce bien utilisateur correspond à la clef privée générée à l'extérieur du produit et fournie au produit. Cette clef privée est associée à un certificat et à la clef publique contenue dans ce certificat. La clef privée doit rester cohérente avec la clef publique correspondante.

Type de protection : confidentialité

4.2 Certificat

Ce bien utilisateur correspond au certificat édité par l'autorité de certification et qui contient en particulier les éléments d'information suivants :

- la désignation de l'autorité de certification émettrice du certificat
- le nom du titulaire de la clé publique
- la valeur de la clé publique
- la période de validité au-delà de laquelle il sera suspendu ou révoqué des informations complémentaires optionnelles :
  - restrictions d'usage des clés (signature, chiffrement, certification ...)
  - politique de certification appliquée pour obtenir le certificat
- la signature du certificat généré par l'autorité de certification

Type de protection : intégrité

4.3 Pin

Ce bien utilisateur correspond au code PIN utilisé pour accéder au périphériques PKCS#11.

Type de protection : confidentialité

4.4 Mot de passe

Ce bien utilisateur correspond à un mot de passe utilisé pour accéder au magasin de certificat logiciel (PKCS12/JKS).

Type de protection : confidentialité

4.5 Alias de clé privée

Ce bien correspond au nom symbolique de la clé privée utilisée dans un boitier de type HSM, cette donnée, peut être connue à l'extérieur du produit (en général des utilitaires permettent d'en connaitre la valeur), toutefois dès lors que l'alias est fourni au produit et durant son éxecution, il ne doit plus être accessible de façon externe au produit.

Type de protection : confidentialité

4.6 Application

Ce bien est nécessaire au fonctionnement du produit et correspond à la partie applicative du produit.

Type de protection : intégrité

Note de sécurité :

Les biens sensibles notés ci-dessus sont pris en charge par le produit, qui en assure la protection telle que décrite, pendant son exécution.

L'application appelante conserve la responsabilité sur ces données en dehors du périmètre du produit (avant et après appel). Toutefois, le guide d'installation du produit indique des recommandations de mise en œuvre de mesures de protection.

5 DESCRIPTION DES MENACES

Les agents menaçants considérés sont des attaquants essayant d'utiliser illégitimement le produit ou essayant de se faire passer pour l'utilisateur légitime du produit auprès de services distants. Les attaques nécessitent le vol préalable du produit ou l'interception de données transitant hors du produit.

Par hypothèse, l'application appelante et l'intégrateur ne sont pas considérés comme des attaquants.

5.1 Menaces relatives à l'authentification utilisateur

5.1.1 Divulgation mot de passe

Connaissance illégitime du mot de passe d'un fichier « magasin de certificat » (PKCS#12, JKS). Cela permet d'accéder à la clef privée pour effectuer une signature, signer un jeton d'horodatage, signer une requête OCSP ou authentifier un client d'un service distant.

5.1.2 Divulgation pincode pour la signature

Connaissance illégitime du pincode permettant d'accéder à un périphérique cryptographique (HSM) de signature.

5.2 Menaces relatives à la gestion des clés

5.2.1 Divulgation clef privée

Accès illégitime à la valeur de la clef privée afin, par exemple, de s'authentifier en tant qu'utilisateur autorisé et de signer un document, un jeton d'horodatage ou une requête OCSP.

5.2.1 Concordance clef privée/certificat

Modification de la clé privée, de son alias sur HSM ou le certificat contenant la clé publique correspondante, permettant ainsi créer une signature électronique invalide par construction.
Ceci tient compte d'une possible erreur de paramétrage, induisant la non concordance.

5.3 Menaces relatives à l'utilisation d'informations de provenance externes

5.3.1 Modification des réponses sur le statut de certificat

Un attaquant peut tenter de forger une réponse incorrecte sur le statut du certificat de signature (CRL ou OCSP)

5.3.1 Modification des réponses sur l'horodatage d'un service

Un attaquant peut tenter de forger une réponse incorrecte et modifier l'heure indiquée dans un jeton d'horodatage.

5.4 Menaces relatives à l'administration du produit

5.4.1 Modification du produit

Le contenu du produit peut être modifié, de tel sorte qu'il ne rende plus le service, ou plus correctement.

6 FONCTIONS DE SECURITE DU PRODUIT

6.1 Protection du code exécutable du produit

La protection doit couvrir les tentatives de modification du produit dans le but de forger un service différent, induisant un comportement différent du fonctionnement nominal.

- Le produit est livré sous la forme d'archive Java (Jar) qui sont signées par un utilitaire standard (Jarsigner) mis en œuvre par le développeur. Toute modification du code est détectée lors du chargement du produit. Le certificat utilisé est émis par une autorité de certification propre. Le guide d'installation décrit la procédure permettant de vérifier les archives java

- Un site web institutionnel décrivant le produit, permet d'obtenir le hash de chacun des composants du produit livré. Le guide d'installation décrit la procédure permettant au l'intégrateur de recalculer ces hash pour les comparer à la valeur sur le site web.

6.2 Protection des biens sensibles en confidentialité

La protection doit permettre d'empêcher la divulgation des biens sensibles en dehors des utilisateurs légitimes

- Les objets dont la protection en confidentialité a été déterminée, sont brouillés en mémoire lorsqu'ils ne sont pas utilisés directement par le produit

- Lors du brouillage un code de vérification est ajouté à la donnée brouillée, afin de vérifier le fonctionnement correct lors du débrouillage.

- En fin d'exécution du produit, un effacement de ces objets est réalisé par écriture d'une valeur de bourrage dans la zone mémoire correspondante.

- En complément la modification volontaire ou involontaire d'une telle donnée brouillée déclenchera une erreur de fonctionnement remontée par le produit.

6.3 Protection des clés et certificats de cachet serveur

La protection permet de s'assurer que le cachet serveur qui est produit, utilise bien le bon couple clé privée de cachet serveur / certificat de cachet serveur

- Une vérification de la correspondance clé privée / clé publique est réalisée à chaque utilisation initiale (chargement du service). Pour cela le produit effectue une signature « à blanc » de bas niveau (PKCS#1)

6.4 Protection des informations de provenance externes

La protection permet de s'assurer de la légitimité des informations externes (hors produit et application appelante) obtenues par le produit pour assurer le service.

- Lorsque le produit utilise une CRL ou une réponse OCSP, il vérifie que l'objet est effectivement signé par la même Autorité de certification que l'émetteur de certificat. Le produit ne prend pas en compte une signature par une autorité tierce.

- Lorsque le produit obtient un jeton d'horodatage, il vérifie qu'il est signé par une autorité d'horodatage référencée.

7 Fin du document