Date : 01 Avril 2011

Origine : DES/SEC/Trusty

Dossier : *TRUSTYTIME V2*

Titre : **CIBLE DE SECURITE TRUSTYTIME V2**

Référence : CSSI/HLS/TRUSTY/FR/07/0059 version 1.10

État : ***APPROUVÉ***

22, avenue Galilée – 92350 Le Plessis Robinson – France – Tél. : +33 (0)1 41 28 40 00 – Fax : +33 (0)1 41 28 40 40

TABLE DES MATIÈRES

22, avenue Galilée – 92350 Le Plessis Robinson – France – Tél. : +33 (0)1 41 28 40 00 – Fax : +33 (0)1 41 28 40 40

22, avenue Galilée – 92350 Le Plessis Robinson – France – Tél. : +33 (0)1 41 28 40 00 – Fax : +33 (0)1 41 28 40 40

Références

[CC]	Common Criteria for Information Technology Security Evaluation, version 3.1 revision 2 - Part 1: Introduction and general model, ref. CCMB-2006-09-001 - Part 2: Security functional requirements, ref. CCMB-2007-09-002 - Part 3: Security assurance requirements, ref. CCMB-2007-09-003
[DCSSI_AUTH]	Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, Version 0.13 du 3 avril 2007
[DCSSI_CRYPTO]	Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard, Version 1.10
[DCSSI_GESTION_CLES]	Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques de niveau de robustesse standard, Version 1.0 du 13 mars 2006
[DCSSI_QS]	Processus de qualification d'un produit de sécurité - niveau standard - version 1.0, ref. N°001591/SGDN/DCSSI/SDR, SGDN/DCS SI, 28/07/2003
[PP-SH]	Profil de protection PP2008/07 « Système d'horodatage » version 1.7, réf. PP-SH-CCv3.1, DCSSI
[ETSI TS1]	ETSI TS 101 861: Time stamping profile, v1.2.1, March 2002
[ETSI TS2]	ETSI TS 102 023: Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities, v1.2.1, January 2003
[ITU-R]	ITU-R Recommendation TF.460-5: "Standard-Frequency and Time-signal emissions", 1997
[Certificat Luna]	*Produit en cours de certification*
[MCSO PP]	CEN Workshop Agreement 14167 Cryptographic Module for CSP Signing Operations - Protection Profile

Glossaire

CC	Critères Communs [CC]
CSP	Certification Service Provider
CSP-SCD	CSP Signature Creation Data
OSP	Organisational Security Policy: Politique de sécurité du système dans lequel est exploitée la cible de l'évaluation (la TOE).
ST	Security Target : le présent document
TOE	Target Of Evaluation: il s'agit du produit ou du système dont la présente cible de sécurité constitue le cahier des charges pour l'évaluation.
TSF	TOE Security Functions: Sous-ensemble du produit ou du système à évaluer où sont implémentées les exigences fonctionnelles de sécurité décrites au chapitre 6.1 du présent document.

1. INTRODUCTION

1.1. IDENTIFICATION DE LA CIBLE DE SÉCURITÉ (ST)

Titre	CIBLE DE SECURITE TrustyTime V2 : CSSI/HLS/TRUSTY/FR/07/0059
Version	1.10
Auteur(s)	CSSI
Date	01 Avril 2011

1.2. IDENTIFICATION DE LA CIBLE D'ÉVALUATION (TOE)

Développeur	CS
Nom du produit	TrustyTime
Version	2.1.5

1.3. VUE D'ENSEMBLE DE LA CIBLE D'ÉVALUATION

1.3.1. Type de TOE

TrustyTime est un système d'horodatage permettant d'émettre des jetons d'horodatage fiable, ces jetons fournissent une association de confiance entre un condensé de document (obtenu par application d'une fonction de hachage sur le document à horodater) et une marque de temps. Les jetons d'horodatage interviennent dans la construction de preuve d'existence ou d'antériorité d'un événement ou d'une transaction, de preuve de possession, ou de validité de l'engagement d'un signataire à un instant donné.

TrustyTime est un système d'horodatage fournissant également des fonctionnalités d'archivage, ne faisant pas partie de la TOE et de conservation sur le long terme de la valeur probante des jetons d'horodatage délivrés. TrustyTime peut contribuer efficacement à bâtir des services de non répudiation forte avec fourniture des éléments de preuve dans le temps en cas de contestation ou de litige.

Les fonctionnalités d'archivage ne sont pas couvertes par la TOE.

1.3.2. Utilisation de la TOE

TrustyTime permet de mettre en œuvre une ou plusieurs **unités d'horodatage** identifiables par un nom donné par une Autorité de Certification[1].

Pour représenter l'ensemble des informations permettant de définir une unité d'horodatage, les notions de contextes d'horodatage non opérationnels et opérationnels sont également introduites.

Un **contexte d'horodatage non opérationnel** est défini comme l'ensemble des informations suivantes :

- l'identification de l'horloge interne utilisée pour obtenir la valeur du temps mise dans le jeton d'horodatage,
- la précision garantie pour le temps contenu dans le jeton d'horodatage par rapport au temps

[1] Par conséquent, une unité d'horodatage n'existe pas en tant que telle avant qu'un certificat obtenu auprès d'une Autorité de Certification et permettant cette identification ne soit présent dans le système.

UTC,

- la valeur de la bi-clé (et l'identifiant de l'algorithme à clé publique) pour la création et la vérification de la signature de jetons d'horodatage,
- la durée d'utilisation de la clé privée définie à la création du contexte non opérationnel,
- la ou les références des politiques d'horodatage supportées,
- les identifiants des algorithmes de hachage pour chaque politique d'horodatage. Les identifiants des algorithmes de hachage admis permettent de déterminer les fonctions utilisées pour obtenir le condensé à horodater

Un **contexte d'horodatage opérationnel** regroupe les informations d'un contexte d'horodatage non opérationnel ainsi que les informations suivantes :

- la durée de vie effective de la clé privée du contexte qui est déterminée lors de l'import du certificat (en tenant compte, lorsqu'elle est présente dans le certificat, de l'extension indiquant la période d'utilisation de la clé privée),
- le certificat d'unité d'horodatage obtenu auprès d'une Autorité de Certification.

Une unité d'horodatage peut donc contenir plusieurs contextes non opérationnels, mais ne peut contenir au plus qu'un seul contexte opérationnel à un instant donné.

L'unité d'horodatage utilise les informations du contexte opérationnel et la valeur d'une horloge interne synchronisée avec UTC. La synchronisation de l'horloge interne d'une unité d'horodatage avec UTC repose sur :

- la synchronisation initiale de l'horloge interne lors de la phase d'initialisation de l'unité d'horodatage par rapport à une source de temps dont la précision est connue par rapport à une source UTC(k),
- le suivi de la dérive de l'horloge interne et le maintien de la synchronisation par rapport à un temps de référence durant la vie normale de l'unité d'horodatage.

Le temps de référence est une approximation locale du temps UTC qui est obtenue à partir de plusieurs sources de temps dont la précision est connue par rapport à une ou plusieurs sources UTC(k). L'établissement du temps de référence utilise au minimum trois sources de temps externes non authentifiées de natures différentes (serveurs NTP, sources radio,…) dont les valeurs sont combinées au travers d'un algorithme de décision.

Le suivi de la dérive de l'horloge interne d'une unité d'horodatage repose sur :

- la comparaison de l'horloge interne et du temps de référence de manière à détecter les écarts instantanés importants entre ces deux valeurs,
- la vérification de la synchronisation de l'horloge interne pour son éventuelle synchronisation qui exploite un historique des écarts entre l'horloge interne et le temps de référence de manière à détecter les variations lentes de l'écart entre ces deux valeurs.

1.4. DESCRIPTION DE LA TOE

1.4.1. Architecture logique de la TOE

La Figure 1 présente les composants fonctionnels qui constituent la TOE au niveau logique. Le périmètre fonctionnel de la TOE est défini par les composants en grisé.

L'authentification locale applicative de l'Administrateur de sécurité et de l'Auditeur sur une unité d'horodatage fait partie du périmètre de la TOE, les tunnels SSH et SSL intervenant dans la création du canal de sécurité entre les clients et la TOE sont hors périmètre de la TOE.

Les fonctions de supervision, le HSM cryptographique, et la station de supervision elle-même ne sont pas considérées dans le périmètre de la TOE.

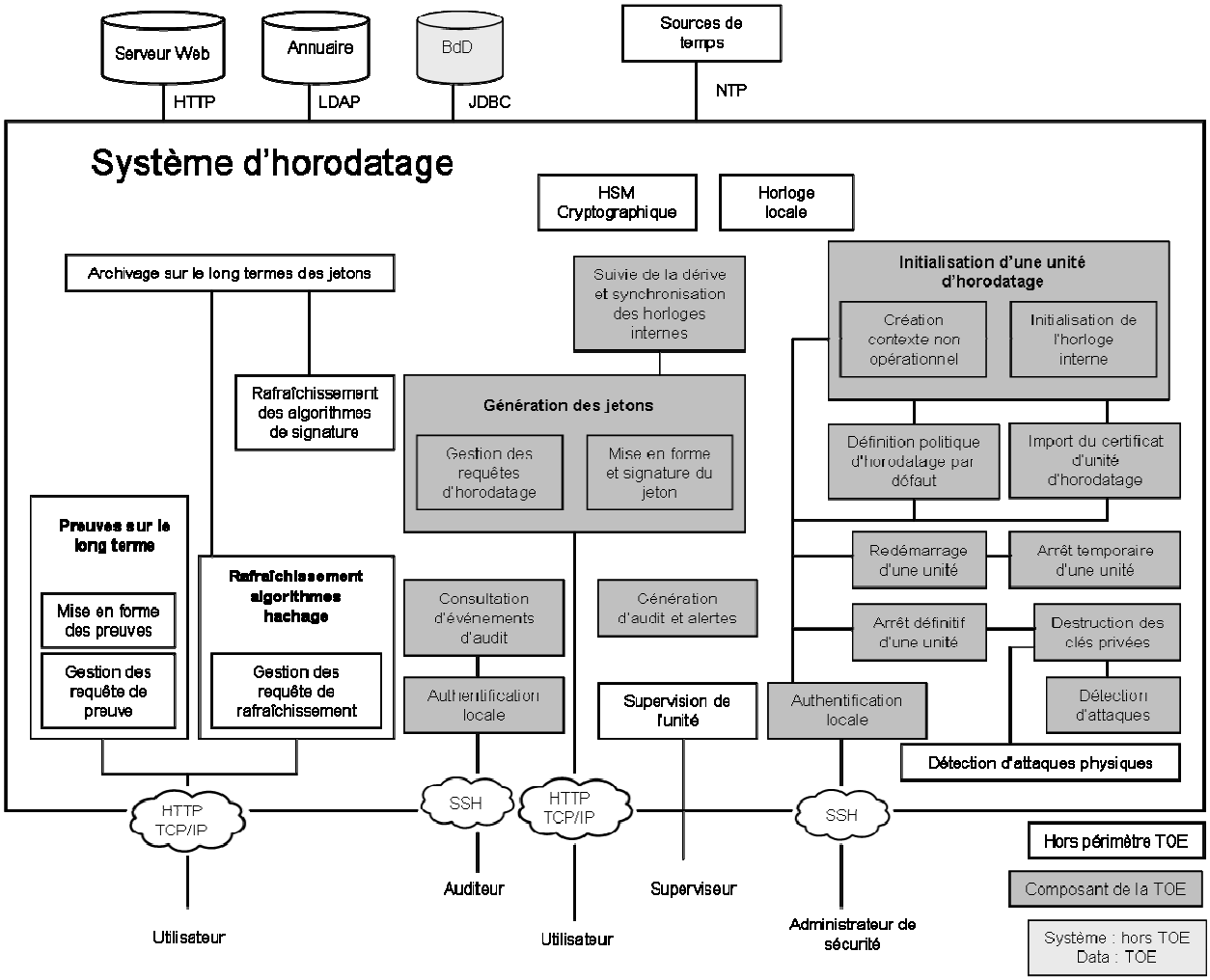

Figure 1 : Architecture logique du système d'horodatage

La détection d'attaques physiques, l'audit des transactions d'horodatage elles-mêmes et l'accès à ces transactions par un Administrateur ne sont pas considérés comme faisant partie du périmètre de la TOE.

1.4.2. Périmètre de la TOE

1.4.2.1. Services fournis par la TOE

Génération des jetons d'horodatage

Le service principal offert par la TOE concerne la génération des jetons d'horodatage. Ces jetons correspondent à l'association signée d'un condensé de document, de la date et heure de l'horloge interne d'une unité d'horodatage, de la référence non ambiguë du certificat d'unité d'horodatage, et de la politique d'horodatage utilisée.

Une des interfaces de la TOE permet de recevoir des requêtes de jetons d'horodatage qui doivent contenir le condensé du document à horodater, la référence à la fonction de hachage utilisée et, de manière optionnelle, l'identifiant de la politique d'horodatage demandée et un nombre unique. Lorsque l'identifiant de la politique d'horodatage n'est pas spécifié dans la requête, une politique d'horodatage par défaut doit être utilisée. Le système traitant la requête de jeton doit vérifier que la fonction de hachage référencée dans la requête est bien autorisée par la politique d'horodatage utilisée, et que la longueur du condensé est adéquate pour l'algorithme en question.

Si l'unité d'horodatage supportant la politique demandée dans la requête ou la politique par défaut est créée dans le système (i.e., la référence de la politique demandée ou de la politique par défaut est présente dans le contexte d'horodatage correspondant), elle génère directement les jetons d'horodatage. Le protocole utilisé doit être à même d'assurer que la réponse correspond bien à la requête qui vient d'être effectuée.

1.4.2.2. Services nécessaires au bon fonctionnement de la TOE

Les services secondaires mais nécessaires au bon fonctionnement de la TOE sont les suivants :

Définition de la politique d'horodatage par défaut

Si la requête de jeton d'horodatage ne spécifie pas de politique d'horodatage, une politique d'horodatage par défaut devra être utilisée. A ce titre, l'Administrateur de sécurité devra définir la politique d'horodatage par défaut sous la forme d'un identifiant de politique d'horodatage, ainsi que les algorithmes de hachage admis pour cette politique.

Initialisation d'une unité d'horodatage

L'initialisation d'une unité d'horodatage consiste à générer la paire de clés qui sera utilisée pour un contexte d'horodatage donné, à synchroniser l'horloge interne par rapport à UTC, à définir la ou les politiques d'horodatage supportées, à définir les algorithmes de hachage admises pour chaque politique d'horodatage, et à définir la durée d'utilisation de la clé privée. Elle nécessite la présence d'un Administrateur de sécurité. Le réglage initial de l'horloge et la génération des clés peuvent être effectués dans un ordre quelconque.

L'initialisation commence par la création d'un contexte non opérationnel qui comprend les informations suivantes :

1. l'identification de l'horloge interne utilisée pour obtenir la valeur du temps mise dans le jeton d'horodatage,
2. la précision garantie pour le temps contenu dans le jeton d'horodatage par rapport au temps UTC,
3. la valeur de la bi-clé (et l'identifiant de l'algorithme),
4. la durée d'utilisation de la clé privée,
5. la ou les références des politiques d'horodatage supportées,
6. les identifiants des algorithmes de hachage pour chaque politique d'horodatage.

A l'issue de cette phase, l'horloge interne est maintenue synchronisée uniquement à l'aide de son algorithme de synchronisation et les informations précédentes ne sont pas modifiables individuellement et ne peuvent être que globalement effacées. Ces informations sont utilisées pour faire une demande de certificat d'unité d'horodatage auprès d'une Autorité de Certification pour ce contexte non opérationnel.

Import des certificats

Il doit être possible d'associer un certificat de clé publique à un contexte non opérationnel. A l'issue de cette opération, le contexte devient opérationnel à condition que la clé publique figurant dans le certificat corresponde bien à la clé publique déjà présente dans le contexte. Cette opération nécessite la présence d'un Administrateur de sécurité.

En ce qui concerne la période d'utilisation effective de la clé privée :

- Soit le certificat contient une extension permettant de connaître la période d'utilisation de la clé privée. Dans ce cas, la durée d'utilisation de la clé privée qui avait été introduite pendant la phase d'initialisation est ignorée, et la valeur contenue dans l'extension est prise en compte en tant que période d'utilisation effective de la clé privée.
- Soit le certificat ne contient pas une extension permettant de connaître la période d'utilisation de la clé privée. Dans ce cas, la durée d'utilisation de la clé privée qui avait été introduite pendant la phase d'initialisation est prise en compte en tant que période d'utilisation effective de la clé privée.

Mise en route et remise en route

Le redémarrage d'une unité d'horodatage en cas de coupure de courant est automatique si toutes les conditions de synchronisation et de sécurité sont réunies lors de la reprise du secteur. Dans le cas contraire, la remise en route nécessite la présence d'un Administrateur de sécurité.

Le redémarrage d'une unité d'horodatage en cas d'arrêt automatique est possible lorsque le contexte opérationnel associé n'a pas été définitivement arrêté (suite à une détection d'attaque par exemple). Le redémarrage nécessite dans ce cas la présence d'un Administrateur de sécurité.

En outre, il doit également être possible de mettre en route ou de remettre en route une unité d'horodatage durant sa vie normale. Cette opération doit pouvoir être effectuée par un Opérateur.

Arrêt temporaire

Les évènements suivants entraînent l'arrêt temporaire automatique d'une unité d'horodatage :

- coupure de courant,
- écart instantané entre l'horloge interne de l'unité d'horodatage et le temps de référence supérieur à une valeur autorisée,
- historique des écarts entre l'horloge interne de l'unité d'horodatage et le temps de référence non conforme à la dérive autorisée sur une période de temps donnée.

En outre, il doit également être possible d'arrêter temporairement une unité d'horodatage durant sa vie normale. Cette opération doit pouvoir être effectuée par un Opérateur.

Arrêt définitif

L'arrêt définitif d'un contexte correspond généralement à la fin de validité de la clé privée de ce contexte. A la fin de sa période de validité, la clé privée du contexte est automatiquement détruite.

L'arrêt définitif de contexte peut également résulter d'une détection d'attaques sur le système d'horodatage qui doit entraîner la destruction de toutes les clés privées des différents contextes.

L'arrêt définitif d'un contexte peut enfin être réalisé sur demande de l'Administrateur de sécurité.

Synchronisation des horloges internes avec UTC

Ce service permet d'assurer le suivi de la dérive des horloges internes d'unité d'horodatage et leur synchronisation avec UTC.

La synchronisation de l'horloge interne d'une unité d'horodatage avec UTC repose sur :

- la synchronisation initiale de l'horloge interne lors de la phase d'initialisation de l'unité d'horodatage par rapport à une source de temps dont la précision est connue par rapport à une source UTC(k),
- le suivi de la dérive de l'horloge interne et le maintien de la synchronisation par rapport au temps de référence durant la vie normale de l'unité d'horodatage.

Le suivi de la dérive de l'horloge interne d'une unité d'horodatage par rapport au temps de référence repose sur :

- la comparaison de l'horloge interne et du temps de référence de manière à détecter les écarts instantanés importants entre ces deux valeurs,
- la vérification de la synchronisation de l'horloge interne pour son éventuelle synchronisation qui exploite l'historique des écarts entre l'horloge interne et le temps de référence de manière à détecter les variations lentes de l'écart entre ces deux valeurs.

La synchronisation et le maintient de l'horloge est gérée au niveau système par l'utilisation de processus de synchronisation standard NTP.

Un suivi supplémentaire, applicatif est mis en place, permet uniquement de vérifier le maintient de la synchronisation de l'horloge interne ainsi que la mise en place de données d'audit protégées.

Génération d'audit et d'alertes

Ce service permet de surveiller et tracer toutes les opérations relatives à l'administration des unités d'horodatage et au maintien de la synchronisation des horloges internes avec UTC.

Des alertes de sécurité sont générées dans les cas suivants :

- détection d'attaques sur les unités d'horodatage,
- écart instantané entre l'horloge interne d'une unité d'horodatage et le temps de référence supérieur à une valeur autorisée,
- historique des écarts non conforme à la dérive autorisée sur une période de temps donnée,

Détection d'attaques

Ce service permet de réagir face à des attaques conduites sur le système d'horodatage visant à divulguer les clés privées des unités d'horodatage. En cas de détection d'attaques, les clés privées des différents contextes doivent être automatiquement détruites.

Authentification locale

Les administrateurs de sécurité et les auditeurs peuvent s'authentifier sur la TOE par l'intermédiaire du protocole SSH.

Consultation/suppression des évènements d'audit

Les auditeurs peuvent consulter et supprimer si besoin, et après authentification, des évènements d'audit.

Destruction des clés privées

En cas de détection d'attaques, les clés privées des différents contextes sont automatiquement détruites.

1.4.3. Rôles

Le fonctionnement de la TOE dans son environnement opérationnel fait appel directement ou indirectement aux rôles décrits ci-dessous.

Administrateur de sécurité

Administrateur local de la sécurité de la TOE, son rôle est de définir la politique d'horodatage par défaut, d'initialiser les unités d'horodatage, et de les remettre en route en cas d'arrêt automatique pour lesquels un redémarrage automatique n'est pas possible pour des raisons de sécurité.

Auditeur

Administrateur de la politique d'audit, son rôle est de définir les événements à tracer et d'analyser les événements d'audit concernant l'administration des unités d'horodatage et les synchronisations des horloges internes.

Opérateur

Opérateur de la TOE, son rôle est d'assurer le bon fonctionnement du système tant que les conditions de sécurité restent réunies (en assurant par exemple la remise en route suite à une coupure de courant). Il est responsable du maintien en condition opérationnelle de la TOE dans le système d'information au sein duquel elle se trouve.

Utilisateur

Utilisateur de la TOE, son rôle est de soumettre des requêtes contenant les condensés de documents à horodater et l'identifiant de la fonction de hachage utilisée pour obtenir le condensé. Il doit également vérifier la validité du jeton d'horodatage délivré et s'assurer que le certificat d'unité d'horodatage correspondant est en cours de validité et n'a pas été révoqué.

Superviseur

Superviseur (local ou distant) de la TOE, son rôle est de vérifier le bon fonctionnement du système. La supervision de la TOE peut être effectuée à distance.

Dans la suite du document, le terme **Administrateurs** regroupera les rôles : **Administrateur de sécurité et Auditeur.**

1.4.4. Interfaces externes de la TOE

Les interfaces externes de la TOE sont :

1. Interface utilisateur :
    a. implémentation du protocole TSP (TimeStamp Protocole) de la RFC 3161, cette implémentation est réalisée en mode http et/ou socket TCP (en format ASN1),
    b. implémentation d'un protocole, basé sur HTTP/HTTPS, pour la gestion des requêtes de rafraîchissement des algorithmes de hachage.

2. Interface de synchronisation du temps : il s'agit de l'interface avec un référentiel de temps pour synchroniser l'horloge locale à l'aide du protocole NTP. Le protocole NTP (« Network Time Protocol ») est standardisé par l'IETF et il est défini dans la RFC 1305.
3. Interface IGC : c'est l'interface permettant :
   - l'exportation de la clé publique pour la génération des requêtes de certificats d'horodatage (requête pkcs#10) et l'importation hors ligne des certificats en format pkcs#7,
   - LDAP pour l'interrogation des annuaires des certificats et des CRL de l'autorité de certification (responsable de l'émission des certificats d'horodatage),
   - http pour la récupération des CRLs suites aux traitements des extensions CRLDP dans les certificats.
4. Interface d'administration : cette interface permet la création d'un tunnel SSH pour l'administration du boîtier et des applications installées à partir de poste d'administration,
5. Interface base de données : la TOE utilise les services de stockage de la base de données via l'interface JDBC
6. Interface cryptographique : la TOE utilise un HSM cryptographique via une interface JCE/JCA.
7. Interface fichier : la TOE manipule des fichiers (certificat, configuration, contexte non opérationnel, journaux, alertes)
8. Interface supervision : cette interface permet la transmission de trap SNMP V1 à une station de supervision

22, avenue Galilée – 92350 Le Plessis Robinson – France – Tél. : +33 (0)1 41 28 40 00 – Fax : +33 (0)1 41 28 40 40

1.4.5. Environnement matériel et logiciel de la TOE

Pour la sécurité de la TOE, les unités d'horodatage et les équipements d'administration doivent se trouver dans un endroit sûr et leurs accès doivent être contrôlés. Le mode d'administration privilégié est l'administration locale, L'administration à distance du système d'horodatage est optionnelle, elle s'effectue sur un réseau dédié et ne fait pas partie de la TOE. Une supervision du système d'horodatage est possible via une station distante mais celle-ci ne fait pas partie du périmètre de la TOE.

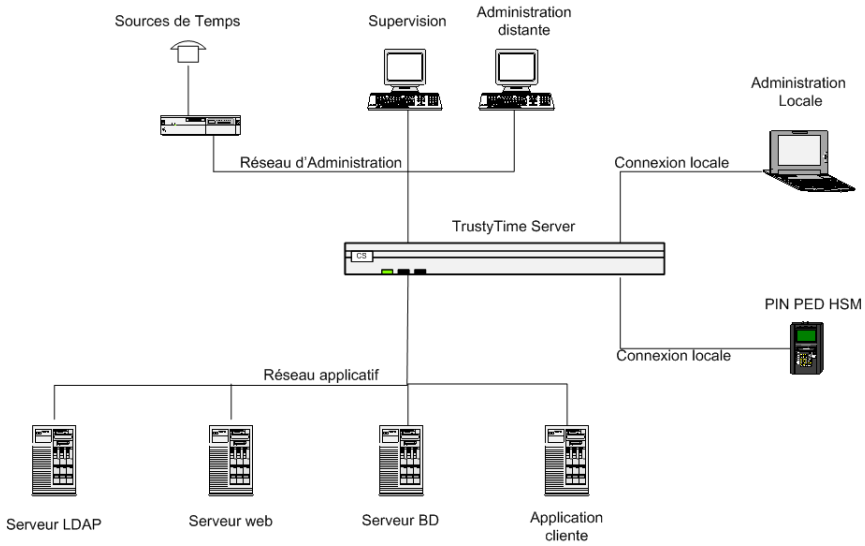

Figure 2 : Architecture physique du système d'horodatage

La TOE s'exécute dans un boîtier fournissant un environnement matériel et logiciel sûr, les caractéristiques de l'environnement pour l'évaluation TrustyTime sont :

- un HSM Cryptographique évaluée Fips 140-2 level 3, et critères communs EAL4+ selon le profil de protection [MCSO PP]. L'évaluation de TrustyTime est réalisée en utilisant le boîtier HSM Luna SP de la société SafeNet
- le système d'exploitation fournit par le boitier Luna SP (à base d'un Linux RedHat 7.2),
- la Java Run Time Environnement v5.0 pour l'exécution de la TOE : JDK 1.5.07,
- un serveur SSH pour la création d'un tunnel sécurisée d'administration
- un serveur Apache Tomcat 5.5.16

Les autres composants faisant partie de l'environnement de la TOE et nécessaire pour son fonctionnement sont :

- la base de données : aucune hypothèse de sécurité n'est faite sur la base de données, l'ensemble des données sensibles de la TOE stockées dans la base de données sont protégés en confidentialité et en intégrité par les fonctions de sécurité de la TOE. Les clés utilisées pour le chiffrement et le scellement des données sont gérées par la TOE dans le HSM cryptographique.
- Les annuaires LDAP et/ou serveurs Web utilisés pour la récupération des données de validation du certificat d'horodatage,
- Les clients SSH (type « Putty ») pour l'administration de la TOE,
- Les Applications clientes d'horodatage conforme à la RFC 3161,

1.4.6. Environnement opérationnel de la TOE

Pour la sécurité de la TOE, le boîtier et ses stations d'administration doivent se trouver dans un endroit sûr et leurs accès doivent être contrôlés.

De la même façon, une infrastructure réseaux doit être mise en place pour filtrer les requêtes envoyées au système et ainsi éviter une saturation due à un envoi d'un nombre anormalement élevé de requêtes.

22, avenue Galilée – 92350 Le Plessis Robinson – France – Tél. : +33 (0)1 41 28 40 00 – Fax : +33 (0)1 41 28 40 40

2. DÉCLARATION DE CONFORMITÉ

2.1. CONFORMITÉ AUX CRITÈRES COMMUNS

Cette cible de sécurité est **strictement conforme** à la partie 2 des Critères Communs version 3.1 révision 2 [CC].

Cette cible de sécurité est **strictement conforme** à la partie 3 des Critères Communs version 3.1 révision 2 [CC].

2.2. CONFORMITÉ À UN PROFIL DE PROTECTION

Cette cible de sécurité ne se réclame conforme à aucun profil de protection même s'il s'inspire largement du profil de protection *Système d'horodatage* [PP-SH] édité par la DCSSI.

2.3. CONFORMITÉ À UN PAQUET D'ASSURANCE

Le niveau d'assurance visé par l'évaluation est EAL3 augmenté du composant ALC_FLR.3.

Ce paquet d'assurance permet de garantir, par une analyse indépendante, que la TOE satisfait les exigences requises :

- En contrôlant les procédures de génération et d'installation de la TOE.
- En vérifiant que les fonctions de sécurité du système sont correctement spécifiées.
- En vérifiant les tests fonctionnels du concepteur et en procédant à des tests indépendants sur la TOE.
- En procédant à des tests de vulnérabilité sur la TOE.

22, avenue Galilée – 92350 Le Plessis Robinson – France – Tél. : +33 (0)1 41 28 40 00 – Fax : +33 (0)1 41 28 40 40

3. DÉFINITION DU PROBLÈME DE SÉCURITÉ

Ce chapitre précise les aspects de sécurité de l'environnement dans lequel il est prévu d'utiliser la TOE.

3.1. BIENS

3.1.1. Données utilisateur protégées par la TOE

Requêtes de jetons d'horodatage (D.REQUETE)

La requête correspond à la demande envoyée au système d'horodatage pour l'obtention d'un jeton d'horodatage. Elle doit contenir les informations suivantes:

- le condensé du document à horodater,
- l'identifiant de l'algorithme de hachage utilisé pour obtenir ce condensé.

Le condensé du document correspond à l'empreinte obtenue en appliquant au document à horodater un algorithme de hachage qui doit être autorisé par la politique d'horodatage utilisée. L'interface au système d'horodatage ne permet de passer que le condensé d'un document, et pas le document lui-même.

Protection: intégrité.

Jetons d'horodatage (D.JETON)

Le jeton d'horodatage correspond à l'association d'un condensé de document et d'une marque de temps UTC. Le jeton est signé par la clé privée en cours de validité du contexte opérationnel d'une unité d'horodatage.

Protection: intégrité et authentification d'origine.

3.1.2. Données sensibles de la TOE

Contextes d'horodatage (D.CONTEXTES_NON_OPERATIONNELS)

Ce bien correspond à l'association des informations suivantes:

- l'identification de l'horloge interne utilisée pour obtenir la valeur du temps inséré dans le jeton d'horodatage,
- la précision garantie pour le temps inséré dans le jeton d'horodatage par rapport au temps UTC,
- la valeur du bi-clé (et l'identifiant de l'algorithme à clé publique) pour la création et la vérification de la signature de jetons d'horodatage,
- la durée d'utilisation de la clé privée définie à la création du contexte,
- la ou les références des politiques d'horodatage supportées,
- les identifiants des algorithmes de hachage pour chaque politique d'horodatage.

Protection: intégrité et confidentialité pour la clé privée du contexte.

Horloge interne (D.HORLOGE_INTERNE)

Ce bien représente l'horloge interne d'une unité d'horodatage qui fournit la date et l'heure correspondant au temps UTC servant à horodater les jetons.

Protection: intégrité et synchronisation avec UTC.

Politique d'horodatage (D.ID_POLITIQUE)

Les politiques d'horodatage sont déterminées lors de la phase de création d'un contexte non opérationnel. Ils permettent de définir les règles applicables par la TOE et son environnement. Plusieurs contextes non opérationnels pouvant supporter des politiques d'horodatage différentes peuvent être créés dans le système.

Protection: intégrité.

Certificat (D.CERTIFICAT)

Ce bien correspond au certificat de la clé publique associée à la clé privée de signature utilisée par un contexte d'horodatage opérationnel. Le certificat est signé par une Autorité de Certification.

Protection: intégrité et authentification d'origine.

Durée utilisation clé privée signature (D.DUREE_UTIL_CLE_PRIV_SIGN)

Ce bien représente la durée d'utilisation effective de la clé privée d'un contexte opérationnel. Deux cas peuvent se présenter:

1. le certificat de la clé publique associée (D.CERTIFICAT) contient une extension permettant de connaître la période d'utilisation de la clé privée. Dans ce cas, la durée d'utilisation de la clé privée qui avait été introduite pendant la phase d'initialisation est ignorée, et la valeur contenue dans l'extension est prise en compte,
2. le certificat de la clé publique associée (D.CERTIFICAT) ne contient pas une extension permettant de connaître la période d'utilisation de la clé privée. Dans ce cas, la durée d'utilisation de la clé privée qui avait été introduite pendant la phase d'initialisation est prise en compte.

Protection: intégrité.

Durée de robustesse des algorithmes (D.CRYPTO.PERIODE)

Ce bien représente la durée de robustesse présumée de l'algorithme de signature ou de hachage.

Protection: intégrité

Données authentification (D.DONNEES_AUTH_ADMIN)

Ce bien représente les données d'identification et d'authentification utilisées par les administrateurs pour s'authentifier sur la TOE.

Protection: confidentialité et intégrité.

Etat alimentation (D.ETAT_ALIM)

Ce bien permet de déterminer l'état d'alimentation d'une unité d'horodatage:

- fonctionnement grâce à une alimentation externe,
- horloge interne maintenue grâce à une alimentation interne à l'unité d'horodatage dans une plage de fonctionnement normal (suite à une perte d'alimentation),
- horloge interne maintenue grâce à une alimentation interne à l'unité d'horodatage hors de la plage de fonctionnement normal (niveau d'alimentation insuffisant pour maintenir la protection des clés et de l'horloge).

Protection: intégrité.

Etat synchronisation (D.ETAT_SYNCHRO)

Ce bien permet de connaître l'état de synchronisation courant de l'horloge interne d'une unité d'horodatage.

Protection: intégrité.

Audit (D.AUDIT)

Ce bien correspond aux évènements d'audit associés à l'administration de la TOE et aux vérifications de la synchronisation de l'horloge interne d'une unité d'horodatage. Les évènements d'audit relatifs à la vérification de la synchronisation de l'horloge interne concernent:

- la date et la valeur de la dernière comparaison correcte entre l'horloge interne et le temps de référence afin, le cas échéant, de pouvoir détecter un incident lors de la vérification de synchronisation suivante avec une source de temps de référence,

Protection: intégrité et disponibilité.

Alertes (D.ALERTES)

Ce bien correspond aux alertes de sécurité générées par l'unité d'horodatage. Des alertes sont générées dans les cas suivants:

- détection d'attaques sur une unité d'horodatage,
- répétition d'un écart instantané entre l'horloge interne d'une unité d'horodatage et le temps de référence supérieur à une valeur d'alerte autorisée,
- écart instantané entre l'horloge interne d'une unité d'horodatage et le temps de référence supérieur à une valeur autorisée,
- historique des écarts non conforme à la dérive autorisée sur une période de temps donnée,

Protection: intégrité et disponibilité.

3.2. HYPOTHÈSES

3.2.1. Hypothèses sur l'usage attendu de la TOE

A.ADMIN

Les administrateurs sont des personnes non hostiles et compétentes qui disposent des moyens nécessaires à la réalisation de leurs tâches. Ils sont formés pour exécuter les opérations dont ils ont la responsabilité et suivent les manuels et procédures d'administration qui incluent la maintenance du système d'horodatage

A.AUDIT

Il est supposé que l'auditeur consulte régulièrement les événements d'audit générés par la TOE.

A.VERIF_JETON

Il est supposé que l'utilisateur du service principal de la TOE valide et conserve les jetons d'horodatage délivrés par le système d'horodatage. La validation du jeton inclut la vérification:

- de la signature du jeton,

- de la validité du certificat d'unité d'horodatage,

- de la correspondance du condensé horodaté avec le condensé transmis dans la requête.

3.2.2. Hypothèses sur l'environnement opérationnel de la TOE

A.AUTORITE_CERT

Il est supposé que les Autorités de Certification délivrant les certificats des unités d'horodatage mettent en œuvre des pratiques conformément à une politique de certification approuvée par l'autorité responsable du service d'horodatage. Ces pratiques couvrent les activités relatives à la délivrance et à la révocation de ces certificats.

A.AUTORITE_HORODATAGE

Il est supposé que l'autorité qui est responsable du service d'horodatage fourni par la TOE applique les règles définies par les politiques d'horodatage spécifiées dans les contextes d'horodatage.

A.LOCAL

Les équipements constituant la TOE doivent se trouver dans des locaux sûrs à accès contrôlé de manière à empêcher tout accès physique non autorisé.

A.LOCAL_ADMIN

Il est supposé que l'administration de la TOE soit effectuée localement depuis l'environnement sécurisé à accès contrôlé dans lequel se trouve la TOE.

A.RESEAU

Il est supposé que le réseau sur lequel est connecté la TOE est déployé et administré conformément à une politique d'interconnexion de réseau assurant le filtrage des flux rentrants.

A.SUPERVISION

Il est supposé que l'environnement de la TOE permette de superviser à distance l'état opérationnel du système d'horodatage.

A.TEMPS_REFERENCE

Il est supposé qu'il sera procédé, au moment de l'initialisation d'une unité d'horodatage, à une vérification de la bonne initialisation du temps de référence.

Il est supposé de plus qu'aucune attaque ne puisse compromettre simultanément et de manière cohérente les valeurs d'une horloge interne d'unité d'horodatage et du temps de référence.

3.3. MENACES

Les menaces présentes dans cette section sont uniquement des menaces qui portent atteinte à la sécurité de la TOE et non aux services rendus par la TOE, car tous les éléments de l'environnement concernant les services rendus par la TOE sont considérés comme des politiques de sécurité organisationnelles.

Les différents agents menaçants sont:

- les attaquants internes: toute personne autorisée à accéder à l'environnement contrôlé de la TOE (Opérateurs par exemple).
- les attaquants externes: toute personne extérieure à l'environnement contrôlé de la TOE (Utilisateurs du service d'horodatage par exemple).

Les administrateurs ne sont considérés comme des attaquants seulement dans le cas d'erreurs involontaires (hypothèse A.ADMIN).

3.3.1. Menaces portant sur les contextes d'horodatage

T.MODIF_CONTEXTE

Un attaquant interne modifie de manière non autorisée les informations suivantes faisant partie d'un contexte d'horodatage:

- l'identification de l'horloge interne de manière à utiliser une horloge interne moins précise,

- la précision garantie pour le temps contenu dans le jeton d'horodatage par rapport au temps UTC de manière à améliorer la précision qui peut être indiquée dans le jeton d'horodatage,

- la valeur de la clé privée de manière à créer une situation de déni de service,

- la valeur de la clé publique de manière à faire certifier une clé publique dont la clé privée est connue ou à créer une situation de déni de service,

- la durée d'utilisation de la clé privée définie à la création du contexte de manière à conserver la clé privée pour une durée plus longue que celle initialement prévue,

- la durée d'utilisation effective de la clé privée de manière à conserver la clé privée pour une durée plus longue que celle calculée en fin d'initialisation de l'unité d'horodatage,

- la ou les références des politiques d'horodatage supportées de manière à référencer des politiques qui garantissent une précision d'horloge meilleure que celle de l'horloge interne utilisée ou qui autorisent des algorithmes de hachage plus faibles,

- les identifiants des algorithmes de hachage pour chaque politique d'horodatage de manière à référencer des algorithmes de hachage plus faibles,

- le certificat de l'unité d'horodatage de manière à mettre un certificat avec une période de validité ou une durée de validité de clé privée plus longue, ou à créer une situation de déni de service.

3.3.2. Menaces portant sur l'horloge interne d'une unité d'horodatage

T.MODIF_HISTORIQUE_ECARTS

Un attaquant interne modifie l'historique des écarts entre l'horloge interne d'une unité d'horodatage et une source de temps de référence pour qu'une dérive de l'horloge interne ne soit ni détectée ni prise en compte lors de la vérification de synchronisation.

T.MODIF_HORLOGE

Un attaquant interne modifie l'horloge interne d'une unité d'horodatage de manière à obtenir des jetons anti-datés ou post-datés générés avec un temps de référence dont l'écart avec UTC ne vérifie pas la précision requise par la politique d'horodatage utilisée.

Cette modification peut résulter:

- d'une attaque directe sur l'horloge interne d'une unité d'horodatage,

- d'une attaque indirecte sur l'horloge interne en modifiant le temps de référence qui sera pris en compte dans l'historique des écarts exploité pour détecter la dérive lente de l'horloge interne.

3.3.3. Menaces portant sur les requêtes de jetons d'horodatage

T.INCOHERENCE_HACHAGE

Un attaquant externe fournit lors d'une requête de jeton d'horodatage:

- un condensé dont la longueur est incohérente avec l'algorithme de hachage référencé, ou

- l'identifiant d'un algorithme de hachage qui n'est pas autorisé par la politique d'horodatage appliquée par l'unité d'horodatage.

T.REQUETE_ERRONNEE

Un attaquant externe compromet l'intégrité des services ou des biens sensibles de la TOE en soumettant une requête mal formée ou de taille erronée au système d'horodatage.

3.3.4. Menaces portant sur les clés cryptographiques

T.DIVULG_CLES

Un attaquant interne divulgue la clé privée d'une unité d'horodatage de manière à:

- usurper l'identité de cette unité d'horodatage lors de la génération ultérieure de jetons, ou

- compromettre des jetons précédemment générés avec cette unité.

T.DIVULG_DONNEES_AUTH_ADMIN

Un attaquant interne divulgue les données d'authentification utilisées par l'Administrateur de sécurité ou l'Auditeur et permet ainsi à une personne non autorisée de s'authentifier sur la TOE.

T.MODIF_DONNEES_AUTH_ADMIN

Un attaquant interne modifie les données d'authentification utilisées par l'Administrateur de sécurité ou l'Auditeur pour créer une situation de déni de service pour les opérations d'administration ou d'audit, ou pour les révéler à une personne qui peut ainsi s'authentifier sur la TOE de manière non autorisée.

3.3.5. Menaces portant sur les états d'une unité d'horodatage

T.MODIF_ETAT_ALIM

Un attaquant interne modifie l'état d'alimentation d'une unité d'horodatage pour maintenir les services de génération de jetons malgré une perte d'alimentation, ou empêcher la destruction des contextes d'horodatage lorsque l'alimentation interne de cette unité d'horodatage sort de sa plage de fonctionnement normal.

T.MODIF_ETAT_SYNCHRO

Un attaquant interne modifie l'état de synchronisation courant de l'horloge interne d'une unité d'horodatage pour maintenir les services de génération de jetons avec un temps de référence dont l'écart avec UTC ne vérifie pas la précision requise par la politique d'horodatage utilisée.

3.3.6. Menaces portant sur l'administration

T.USURP_ADMIN

Un attaquant interne se fait passer pour un Administrateur de sécurité ou un Auditeur et effectue des opérations d'administration ou d'audit non autorisées.

3.3.7. Menaces portant sur l'audit

T.MODIF_AUDIT

Un attaquant interne modifie les enregistrements d'évènements d'audit de manière à effacer des opérations illicites conduites sur le système d'horodatage.

3.4. POLITIQUE DE SÉCURITÉ DE L'ORGANISATION (OSP)

3.4.1. Opérations Cryptographiques

OSP.CRYPTO

Le référentiel de cryptographie tel que défini par la DCSSI [CRYPTO-STD] doit être suivi pour les fonctions de cryptographie utilisées dans la TOE et pour la gestion des clés cryptographiques et données d'authentification de la TOE (identification et authentification des administrateurs, génération des bi-clés, destruction des clés privées, et génération de signature pour les jetons d'horodatage).

3.4.2. Services de sécurité rendus par la TOE

OSP.GESTION_CONTEXTE

La TOE doit permettre:

- la création de contextes d'horodatage non opérationnels par un administrateur de sécurité,

- la consultation des informations définies dans les contextes d'horodatage à l'exception des valeurs des clés privées des différents contextes par un administrateur de sécurité,

- l'arrêt définitif de contextes d'horodatage par un administrateur de sécurité et par la TOE.

OSP.IMPORT_CERTIFICAT

La TOE doit permettre d'importer le certificat correspondant à la bi-clé d'un contexte non opérationnel. La clé publique figurant dans le certificat doit correspondre à la clé publique déjà présente dans le contexte.

OSP.POLITIQUE_HORODATAGE_DEFAUT

La TOE doit permettre de référencer la politique d'horodatage par défaut et les identifiants des algorithmes de hachage autorisés pour cette politique.

OSP.PROTOCOLE_REQUETE

Le protocole mis en œuvre par la TOE pour la gestion des requêtes de jetons d'horodatage doit garantir la présence des éléments de données de la requête dans la réponse délivrée par le système d'horodatage. Ces éléments incluent l'identifiant de l'algorithme de hachage utilisé pour obtenir le condensé du document, la valeur du condensé lui-même et, de manière optionnelle, l'identifiant de la politique d'horodatage demandée et un nombre unique.

Le nombre unique, s'il est présent dans la requête, permet à l'Utilisateur du système d'horodatage de vérifier que la réponse délivrée par le système correspond bien à la requête émise en l'absence d'horloge locale chez l'Utilisateur.

OSP.SERVICE_RENDU

La TOE doit générer des jetons d'horodatage conformément à la politique d'horodatage utilisée. Les jetons d'horodatage sont signés par la clé privée du contexte opérationnel de l'unité d'horodatage qui les génère et ils doivent au minimum inclure les éléments suivants:

- le condensé du document et l'identifiant de l'algorithme de hachage utilisé pour l'obtenir,

- le temps fourni par l'horloge interne de l'unité d'horodatage utilisée dont la précision par rapport au temps UTC est garantie,

- la référence non ambiguë du certificat d'unité d'horodatage,

- la référence de la politique d'horodatage utilisée.

OSP.SYNCHRO_HORLOGE_INTERNE

La TOE doit assurer le suivi de la dérive de l'horloge interne d'une unité d'horodatage et le maintien de sa synchronisation par rapport au temps UTC durant la vie normale de l'unité d'horodatage. La synchronisation de l'horloge interne d'une unité d'horodatage s'effectue à l'aide d'un algorithme de synchronisation exploitant un historique des écarts entre cette horloge interne et le temps de référence.

22, avenue Galilée – 92350 Le Plessis Robinson – France – Tél. : +33 (0)1 41 28 40 00 – Fax : +33 (0)1 41 28 40 40

4. OBJECTIFS DE SÉCURITÉ

Les objectifs de sécurité reflètent l'intention déclarée et sont à même de contrer toutes les menaces identifiées et de couvrir toutes les politiques de sécurité organisationnelles et les hypothèses identifiées.

4.1. OBJECTIFS DE SÉCURITÉ POUR LA TOE

4.1.1. Génération de jetons d'horodatage

O.GENERATION_JETONS

La TOE doit garantir l'intégrité et l'authentification d'origine des jetons lors de leur délivrance par le système d'horodatage. Les jetons d'horodatage générés doivent au minimum inclure les éléments suivants:

- le condensé du document et l'identifiant de l'algorithme de hachage utilisé l'obtenir,

- le temps fourni par l'horloge interne de l'unité d'horodatage utilisée dont la précision par rapport au temps UTC est garantie,

- la référence non ambiguë du certificat d'unité d'horodatage,

- la référence de la politique d'horodatage utilisée.

Avant de signer un jeton d'horodatage, la TOE doit également garantir que le temps (date et heure) qui doit y être inclus ne soit en aucun cas inférieur au temps qui a été inclus dans le jeton précédemment émis par l'unité d'horodatage utilisée.

O.POLITIQUE_HORODATAGE_DEFAUT

La TOE doit permettre de référencer la politique d'horodatage par défaut et les identifiants des algorithmes de hachage autorisés pour cette politique.

O.PROTOCOLE_REQUETE

La TOE doit implémenter un protocole de gestion des requêtes de jetons d'horodatage garantissant que les réponses délivrées par le système d'horodatage contiennent les éléments de données présents dans les requêtes correspondantes. Ces éléments incluent l'identifiant de l'algorithme de hachage utilisé pour obtenir le condensé du document, la valeur du condensé lui-même et, de manière optionnelle, l'identifiant de la politique d'horodatage demandée et un nombre unique.

O.VERIF_HACHAGE

La TOE doit vérifier, lors d'une requête de jeton d'horodatage, que la longueur du condensé de document à horodater est cohérente avec l'identifiant de l'algorithme de hachage référencé, et que cet algorithme est autorisé pour la politique d'horodatage utilisée.

O.VERIF_REQUETE

La TOE doit vérifier la conformité des requêtes de jetons d'horodatage vis-à-vis du format attendu.

4.1.2. Gestion des contextes d'horodatage

O.ARRET_CONTEXTE

La TOE doit pouvoir arrêter définitivement un contexte d'horodatage et cesser d'utiliser les informations de ce contexte pour fournir les services de génération de jetons d'horodatage dans les cas suivants:

- détection d'attaques sur le système d'horodatage (entraînant l'arrêt définitif de tous les contextes),

- sur demande d'un administrateur de sécurité.

L'arrêt définitif d'un contexte doit entraîner la destruction de la clé privée associée

O.CONSULT_CONTEXTE

La TOE doit permettre à l'administrateur de sécurité de visualiser les informations suivantes contenues dans les différents contextes d'horodatage supportés par le système d'horodatage:

- l'identification de l'horloge interne utilisée pour obtenir la valeur du temps mis dans le jeton d'horodatage,

- la précision garantie pour le temps contenu dans le jeton d'horodatage par rapport au temps UTC,

- la durée d'utilisation de la clé privée définie lors de l'initialisation de l'unité d'horodatage,

- la ou les références des politiques d'horodatage supportées,

- les identifiants des algorithmes de hachage pour chaque politique d'horodatage,

- la durée de vie effective de la clé privée du contexte (pour les contextes opérationnels),

- le certificat d'unité d'horodatage (pour les contextes opérationnels)

O.CREATION_CONTEXTE_NON_OPERATIONNEL

La TOE doit permettre à l'administrateur de sécurité de créer un contexte d'horodatage non opérationnel qui comprend les informations suivantes:

- l'identification de l'horloge interne utilisée pour obtenir la valeur du temps mise dans le jeton d'horodatage,

- la précision garantie pour le temps contenu dans le jeton d'horodatage par rapport au temps UTC,

- la valeur de la bi-clé (et l'identifiant de l'algorithme à clé publique) pour la création et la vérification de la signature de jetons d'horodatage,

- la durée d'utilisation de la clé privée,

- la ou les références des politiques d'horodatage supportées,

- les identifiants des algorithmes de hachage pour chaque politique d'horodatage.

L'ensemble de ces informations, à l'exception de la valeur de la bi-clé, peut être modifié par l'administrateur de sécurité tant que le contexte d'horodatage non opérationnel n'est pas déclaré créé par l'administrateur de sécurité. Les informations d'un contexte d'horodatage non opérationnel déclaré créé ne sont pas modifiables individuellement et ne peuvent être que globalement effacées par l'administrateur de sécurité.

O.PROTECTION_CONTEXTE_OPERATIONNEL

La TOE doit garantir qu'un contexte d'horodatage opérationnel ne puisse pas être modifié. Un contexte d'horodatage opérationnel peut par contre être définitivement arrêté, ce qui entraîne la destruction de la clé privée de ce contexte.

4.1.3. Gestion des clés cryptographiques

O.CRYPTO

La TOE doit implémenter les fonctions de cryptographie et gérer des clés cryptographiques et données d'authentification en accord avec le référentiel de cryptographie défini par la DCSSI [CRYPTO-STD]. La gestion des clés cryptographiques et données d'authentification concerne:

- l'identification et l'authentification des administrateurs,

- la génération des bi-clés utilisées pour créer et vérifier la signature des jetons d'horodatage délivrés par le système d'horodatage,

- la destruction des clés privées des contextes d'horodatage,

- la génération de signature pour les jetons d'horodatage.

O.EXPORT_CLES

La TOE ne doit pas permettre d'exporter les clés privées de signature générées par la TOE.

O.IMPORT_CERTIFICAT

La TOE doit permettre d'importer le certificat de clé publique correspondant à la bi-clé d'un contexte non opérationnel à condition que la clé publique figurant dans le certificat corresponde bien à la clé publique déjà présente dans ce contexte.

O.IMPORT_CLES

La TOE ne doit pas permettre d'importer des clés privées ou des paires de clés de signature générées à l'extérieur de la TOE.

4.1.4. Arrêt d'une unité d'horodatage

O.ARRET_TEMP

La TOE doit arrêter de fournir les services de génération de jetons d'une unité d'horodatage dans les cas suivants:

- état de synchronisation courant de l'horloge interne de l'unité d'horodatage ne permettant pas de garantir la précision requise par la politique d'horodatage utilisée (écart instantané entre l'horloge interne et le temps de référence supérieur à une valeur autorisée ou historique des écarts entre l'horloge interne et le temps de référence non conforme à la dérive autorisée pour une période de temps donnée),

Cet arrêt est temporaire et ne conduit pas à l'arrêt définitif du contexte d'horodatage opérationnel associé.

O.RETOUR_ETAT_SUR

La TOE doit fournir une fonctionnalité permettant de remettre dans un état opérationnel sûr une unité d'horodatage suite à un arrêt temporaire.

4.1.5. Gestion de la synchronisation

O.HORLOGE_INTERNE

La TOE doit assurer la synchronisation des horloges internes d'unité d'horodatage avec UTC avec la précision requise par la politique d'horodatage utilisée. La synchronisation de l'horloge interne d'une unité d'horodatage s'effectue à l'aide d'un algorithme de synchronisation exploitant un historique des écarts entre cette horloge interne et le temps de référence.

4.1.6. Administration

O.AUTH_ADMIN

La TOE doit fournir des mécanismes d'identification et d'authentification des Administrateurs.

4.1.7. Audit et alertes

O.ALERTES

La TOE doit générer une alerte de sécurité pour toute violation potentielle de sécurité, en particulier dans les cas suivants:

- répétition d'un écart instantané entre l'horloge interne d'une unité d'horodatage et le temps de référence supérieur à une valeur d'alerte autorisée,
- mémoire utilisée pour stocker les évènements d'audit proche de sa capacité maximale,
- écart instantané entre l'horloge interne et le temps de référence supérieur à une valeur autorisée,
- historique des écarts entre l'horloge interne et le temps de référence non conforme à la dérive autorisée pour une période de temps donnée.

O.AUDIT_ADMIN

La TOE doit tracer toutes les opérations effectuées par un Administrateur de sécurité sur le système d'horodatage. De plus, elle doit permettre à un Auditeur de consulter ce qui a été tracé.

O.AUDIT_UNITE

La TOE doit tracer toutes les opérations effectuées sur les unités d'horodatage concernant la gestion des contextes d'horodatage et la synchronisation des horloges internes d'unité d'horodatage. De plus, elle doit permettre à un Auditeur de consulter ce qui a été tracé.

Les évènements d'audit relatifs à la synchronisation de l'horloge interne d'une unité d'horodatage concernent:

- les opérations, de niveau système, de vérification de synchronisation nécessaires pour conserver la date et la valeur de la dernière comparaison correcte entre l'horloge interne et le temps de référence,
- les opérations, de niveau système, de synchronisation nécessaires pour conserver la date et la valeur des synchronisations de l'horloge interne,
- les opérations, de niveau applicatif, de vérification de synchronisation nécessaires pour conserver la date et la valeur de la dernière comparaison correcte entre l'horloge interne et le temps de référence,.

Les données d'audit, de niveau système, sont restreintes aux éléments générés par le boitier Luna SP (Cf. [Certificat Luna]).

O.PROTECTION_AUDIT

La TOE doit garantir l'intégrité et la disponibilité des événements d'audit qu'elle enregistre.

4.2. OBJECTIFS DE SÉCURITÉ POUR L'ENVIRONNEMENT OPÉRATIONNEL DE LA TOE

4.2.1. Sécurité physique de l'environnement opérationnel

OE.LOCAL_ADMIN

L'administration de la TOE doit être effectuée localement depuis l'environnement sécurisé à accès contrôlé dans lequel se trouvent les équipements constituant la TOE.

OE.PROTECTION_PHYSIQUE

Les équipements constituant la TOE doivent se trouver dans un local sécurisé à accès contrôlé et limité aux seules personnes autorisées.

4.2.2. Personnel de l'environnement opérationnel

OE.ADMIN

Les administrateurs doivent être formés aux tâches qu'ils ont à réaliser sur la TOE.

4.2.3. Environnement technique opérationnel de la TOE

OE.AUTORITE_CERT

Les Autorités de Certification délivrant les certificats des unités d'horodatage doivent mettre en oeuvre des pratiques conformément à une politique de certification approuvée par l'Autorité d'horodatage. Ces pratiques doivent couvrir les activités relatives à la délivrance et à la révocation de ces certificats.

OE.AUTORITE_HORODATAGE

L'Autorité d'horodatage responsable du service d'horodatage fourni par la TOE doit appliquer les règles définies par les politiques d'horodatage spécifiées dans les contextes d'horodatage.

OE.RESEAU

Le réseau sur lequel est connecté la TOE doit être déployé, configuré et administré conformément à une politique d'interconnexion de réseau assurant le filtrage des flux rentrants.

OE.SUPERVISION

L'environnement de la TOE doit permettre à un Superviseur de consulter à distance l'état opérationnel du système d'horodatage.

4.2.4. Usage de la TOE

OE.ANALYSE_AUDIT

L'Auditeur doit régulièrement analyser les événements d'audit enregistrés par la TOE et agir en conséquence.

OE.DEMANDE_CERTIFICAT

L'Administrateur de sécurité doit vérifier que la demande de certificat d'unité d'horodatage auprès d'une Autorité de Certification contient au moins le sous-ensemble suivant des informations relatives à un contexte non opérationnel:

- la valeur de la clé publique (et l'identifiant de l'algorithme),
- la durée d'utilisation de la clé privée,
- la ou les références des politiques d'horodatage supportées.

OE.IMPORT_CERTIFICAT

L'Administrateur de sécurité doit vérifier, lors de l'import du certificat d'unité d'horodatage, qu'il provient bien d'une Autorité de Certification habilitée à délivrer des certificats pour un contexte donné.

OE.TEMPS_REFERENCE

Les personnels responsables de l'initialisation des unités d'horodatage (incluant un Administrateur de sécurité) doivent procéder, lors de cette initialisation, à une vérification de la bonne initialisation du temps de référence. De plus, l'environnement de la TOE doit garantir qu'aucune attaque ne puisse compromettre simultanément et de manière cohérente les valeurs d'une horloge interne d'unité d'horodatage et du temps de référence.

L'initialisation du temps de référence doit inclure, si cela est applicable, la vérification du chemin de câblage entre l'unité d'horodatage et la ou les sources externes. Dans le cas de sources radio, cette vérification doit également inclure le chemin de câblage des antennes.

Le temps de référence peut s'obtenir de plusieurs manières, par exemple à l'aide:

- d'une source externe unique authentifiée,
- de sources externes multiples non authentifiées,
- d'une horloge atomique située dans l'environnement contrôlé du système d'horodatage.

Le risque d'une compromission simultanée et de manière cohérente des valeurs de l'horloge interne d'une unité d'horodatage et du temps de référence peut par exemple être limité par:

- le choix de technologies différentes (en particulier lorsqu'une horloge atomique fournit le temps de référence, elle ne doit pas également faire fonction d'horloge interne),
- une séparation spatiale.

OE.VERIF_JETON

L'utilisateur du service principal de la TOE doit valider et conserver les jetons d'horodatage délivrés par le système d'horodatage. La validation du jeton inclut la vérification:

- de la signature du jeton,
- de la validité du certificat d'unité d'horodatage,
- de la correspondance du condensé horodaté avec le condensé transmis dans la requête

4.3. ARGUMENTAIRE DES OBJECTIFS DE SÉCURITÉ

4.3.1. Couverture des menaces

4.3.1.1. Menaces portant sur les contextes d'horodatage

T.MODIF_CONTEXTE

Cette menace est contrée par O.CREATION_CONTEXTE_NON_OPERATIONNEL qui garantit que la valeur de la bi-clé d'un contexte d'horodatage non opérationnel ne peut pas être modifiée et que les autres informations d'un contexte non opérationnel ne peuvent être modifiées que par l'administrateur de sécurité tant que le contexte d'horodatage non opérationnel n'est pas déclaré créé. En outre, les informations d'un contexte d'horodatage non opérationnel déclaré créé ne sont pas modifiables individuellement et ne peuvent être que globalement effacées par l'administrateur de sécurité.

O.PROTECTION_CONTEXTE_OPERATIONNEL assure par ailleurs que les informations présentes dans un contexte opérationnel sont non modifiables.

De plus, O.AUTH_ADMIN permet d'assurer que seuls les administrateurs de sécurité authentifiés comme tels peuvent créer des contextes d'horodatage.

O.AUDIT_ADMIN et O.ALERTES couvrent toutes les menaces sur les biens sensibles de la TOE, car ils assurent que les opérations effectuées sur ces biens sensibles sont tracées et que des alertes de sécurité sont générées pour signaler des dysfonctionnements de la TOE de nature accidentelle ou malveillante. Ils permettent ainsi de détecter et de traiter des erreurs ou des attaques après analyse des évènements d'audit et des alertes de sécurité.

4.3.1.2. Menaces portant sur l'horloge interne d'une unité d'horodatage

T.MODIF_HORLOGE

Cette menace est contrée par O.ARRET_CONTEXTES qui assure la destruction du contexte d'horodatage en cas de détection d'attaques sur l'unité d'horodatage. De plus, O.AUTH_ADMIN permet d'assurer que seuls les administrateurs de sécurité authentifiés comme tels peuvent effectuer la synchronisation initiale de l'horloge inclus dans la phase de création d'un contexte d'horodatage.

OE.TEMPS_REFERENCE garantit que la TOE puisse détecter un écart entre l'horloge interne d'une unité d'horodatage et le temps de référence car il assure qu'aucune attaque ne peut compromettre simultanément et de manière cohérente ces deux valeurs.

O.AUDIT_UNITE garantit que toutes les opérations de comparaison entre les valeurs de l'horloge interne d'une unité d'horodatage et du temps de référence et les opérations de synchronisation de l'horloge interne seront tracées pour être consultées par un auditeur.

O.AUDIT_ADMIN et O.ALERTES couvrent toutes les menaces sur les biens sensibles de la TOE, car ils assurent que les opérations effectuées sur ces biens sensibles sont tracées et que des alertes de sécurité sont générées pour signaler des dysfonctionnements de la TOE de nature accidentelle ou malveillante. Ils permettent ainsi de détecter et de traiter des erreurs ou des attaques après analyse des évènements d'audit et des alertes de sécurité.

T.MODIF_HISTORIQUE_ECARTS

Cette menace est contrée par:

O.RETOUR_ETAT_SUR qui couvre les menaces qui modifient ou divulguent les biens sensibles de la TOE de manière non autorisée, car il garantit que la TOE se trouve toujours dans un état sûr.

O.AUDIT_ADMIN et O.ALERTES qui couvrent toutes les menaces sur les biens sensibles de la TOE, car ils assurent que les opérations effectuées sur ces biens sensibles sont tracées et que des alertes de sécurité sont générées pour signaler des dysfonctionnements de la TOE de nature accidentelle ou malveillante.

4.3.1.3. Menaces portant sur les requêtes de jetons d'horodatage

T.REQUETE_ERRONNEE

Cette menace est contrée par O.VERIF_REQUETE qui garantit que la conformité du format de la requête de jeton d'horodatage reçue vis-à-vis du format attendu est vérifiée par la TOE. De plus, O.VERIF_HACHAGE couvre spécifiquement la vérification de la longueur du condensé de document vis-à-vis de l'algorithme de hachage référencé.

T.INCOHERENCE_HACHAGE Cette menace est contrée par O.VERIF_HACHAGE qui garantit la cohérence entre la longueur du condensé de document présent dans la requête de jeton d'horodatage et l'algorithme de hachage référencé. O.VERIF_HACHAGE assure également que l'algorithme de hachage référencé est autorisé par la politique d'horodatage utilisée. De plus, O.VERIF_REQUETE garantit la cohérence globale de la requête reçue vis-à-vis du format attendu.

4.3.1.4. Menaces portant sur les clés cryptographiques

T.DIVULG_CLES

Cette menace est contrée par O.IMPORT_CLES et O.EXPORT_CLES qui garantissent que seules les clés privées générées par la TOE peuvent être utilisées pour signer les jetons d'horodatage, et que ces clés privées ne peuvent être exportées à l'extérieur de la TOE. O.ARRET_CONTEXTES assure que les différents contextes d'horodatage seront arrêtés et que les clés privées de ces contextes seront détruites en cas de détection d'attaques.

O.CRYPTO garantit la bonne gestion des clés cryptographique sur la TOE, y compris lors de la génération de bi-clés et de la destruction de clés privées. De plus, O.AUTH_ADMIN permet d'assurer que seuls les administrateurs de sécurité authentifiés comme tels peuvent effectuer la génération des bi-clés sur la TOE.

O.AUDIT_ADMIN et O.ALERTES couvrent toutes les menaces sur les biens sensibles de la TOE, car ils assurent que les opérations effectuées sur ces biens sensibles sont tracées et que des alertes de sécurité sont générées pour signaler des dysfonctionnements de la TOE de nature accidentelle ou malveillante. Ils permettent ainsi de détecter et de traiter des erreurs ou des attaques après analyse des évènements d'audit et des alertes de sécurité.

T.DIVULG_DONNEES_AUTH_ADMIN

Cette menace est contrée par OE.ADMIN qui assure que les administrateurs de la TOE sont correctement formés pour les tâches qu'ils ont à réaliser sur la TOE et qui requièrent leur identification et leur authentification. De plus, OE.AUTORITE_HORODATAGE garantit que les administrateurs appliquent les règles des politiques d'horodatage supportées par l'Autorité d'horodatage.

OE.LOCAL_ADMIN garantit que l'administration de la TOE ne peut s'effectuer que localement depuis un environnement sécurisé à accès contrôlé.

O.AUDIT_ADMIN et O.ALERTES couvrent toutes les menaces sur les biens sensibles de la TOE, car ils assurent que les opérations effectuées sur ces biens sensibles sont tracées et que des alertes de sécurité sont générées pour signaler des dysfonctionnements de la TOE de nature accidentelle ou malveillante. Ils permettent ainsi de détecter et de traiter des erreurs ou des attaques après analyse des évènements d'audit et des alertes de sécurité.

T.MODIF_DONNEES_AUTH_ADMIN

Cette menace est contrée par OE.ADMIN qui assure que les administrateurs de la TOE sont correctement formés pour les tâches qu'ils ont à réaliser sur la TOE et qui requièrent leur identification et leur authentification. De plus, OE.AUTORITE_HORODATAGE garantit que les administrateurs appliquent les règles des politiques d'horodatage supportées par l'Autorité d'horodatage.

OE.LOCAL_ADMIN garantit que l'administration de la TOE ne peut s'effectuer que localement depuis un environnement sécurisé à accès contrôlé.

O.AUDIT_ADMIN et O.ALERTES couvrent toutes les menaces sur les biens sensibles de la TOE, car ils assurent que les opérations effectuées sur ces biens sensibles sont tracées et que des alertes de sécurité sont générées pour signaler des dysfonctionnements de la TOE de nature accidentelle ou malveillante. Ils permettent ainsi de détecter et de traiter des erreurs ou des attaques après analyse des évènements d'audit et des alertes de sécurité.

4.3.1.5. Menaces portant sur les états d'une unité d'horodatage

T.MODIF_ETAT_ALIM

Cette menace est contrée par O.ARRET_TEMP qui garantit que les services de génération de jetons d'horodatage seront arrêtés en cas de coupure de courant.

O.RETOUR_ETAT_SUR couvre les menaces qui modifient ou divulguent les biens sensibles de la TOE de manière non autorisée, car il garantit que la TOE se trouve toujours dans un état sûr.

O.AUDIT_ADMIN et O.ALERTES couvrent toutes les menaces sur les biens sensibles de la TOE, car ils assurent que les opérations effectuées sur ces biens sensibles sont tracées et que des alertes de sécurité sont générées pour signaler des dysfonctionnements de la TOE de nature accidentelle ou malveillante.

T.MODIF_ETAT_SYNCHRO

Cette menace est contrée par O.ARRET_TEMP qui garantit que les services de génération de jetons d'horodatage seront arrêtés lorsque l'état de synchronisation de l'horloge interne ne permet pas de garantir la précision requise par la politique d'horodatage utilisée.

O.RETOUR_ETAT_SUR couvrent les menaces qui modifient ou divulguent les biens sensibles de la TOE de manière non autorisée, car il garantit que la TOE se trouve toujours dans un état sûr.

O.AUDIT_ADMIN et O.ALERTES couvrent toutes les menaces sur les biens sensibles de la TOE, car ils assurent que les opérations effectuées sur ces biens sensibles sont tracées et que des alertes de sécurité sont générées pour signaler des dysfonctionnements de la TOE de nature accidentelle ou malveillante.

4.3.1.6. Menaces portant sur l'administration

T.USURP_ADMIN

Cette menace est contrée par O.AUTH_ADMIN car cet objectif impose l'authentification des administrateurs avant de pouvoir effectuer des opérations d'administration sur la TOE.

O.AUDIT_ADMIN et O.ALERTES couvrent toutes les menaces sur les biens sensibles de la TOE, car ils assurent que les opérations effectuées sur ces biens sensibles sont tracées et que des alertes de sécurité sont générées pour signaler des dysfonctionnements de la TOE de nature accidentelle ou malveillante. Ils permettent ainsi de détecter et de traiter des erreurs ou des attaques après analyse des évènements d'audit et des alertes de sécurité.

4.3.1.7. Menaces portant sur l'audit

T.MODIF_AUDIT

Cette menace est contrée par O.PROTECTION_AUDIT et O.AUTH_ADMIN qui garantissent l'intégrité des évènements d'audit et imposent que les enregistrements d'évènements d'audit ne puissent être supprimés que par des auditeurs authentifiés comme tels.

22, avenue Galilée – 92350 Le Plessis Robinson – France – Tél. : +33 (0)1 41 28 40 00 – Fax : +33 (0)1 41 28 40 40

O.AUDIT_ADMIN et O.ALERTES couvrent toutes les menaces sur les biens sensibles de la TOE, car ils assurent que les opérations effectuées sur ces biens sensibles sont tracées et que des alertes de sécurité sont générées pour signaler des dysfonctionnements de la TOE de nature accidentelle ou malveillante. Ils permettent ainsi de détecter et de traiter des erreurs ou des attaques après analyse des évènements d'audit et des alertes de sécurité.

4.3.2. Politiques de sécurité organisationnelles (OSP)

OSP.SERVICE_RENDU

Cette OSP est couverte par O.GENERATION_JETONS, O.HORLOGE_INTERNE et O.ARRET_TEMP qui garantissent que la TOE fournit les services de génération de jetons d'horodatage contenant un temps dont la précision par rapport au temps UTC est garantie.

O.CRYPTO couvre également cette OSP car il garantit une bonne gestion des clés lors de la signature des jetons d'horodatage.

OSP.CRYPTO

Cette OSP est couverte par O.CRYPTO pour l'implémentation des fonctions cryptographiques et la gestion des clés cryptographiques et données d'authentification. Elle est également couverte par:

O.AUTH_ADMIN pour l'authentification des administrateurs,

O.GENERATION_JETONS pour la génération de jetons d'horodatage.

OSP.SYNCHRO_HORLOGE_INTERNE

Cette OSP est couverte par O.HORLOGE_INTERNE qui garantit que l'horloge interne d'une unité d'horodatage est maintenue synchronisée avec UTC. De plus, O.AUTH_ADMIN permet d'assurer que seuls les administrateurs de sécurité authentifiés comme tels peuvent effectuer la synchronisation initiale de l'horloge inclus dans la phase de création d'un contexte d'horodatage.

O.AUDIT_ADMIN et O.ALERTES couvrent également cette OSP, car ils assurent que les opérations effectuées sur ces biens sensibles sont tracées et que des alertes de sécurité sont générées pour signaler des dysfonctionnements de la TOE de nature accidentelle ou malveillante. Ils permettent ainsi de détecter et de traiter des erreurs ou des attaques après analyse des évènements d'audit et des alertes de sécurité. De plus, O.AUDIT_UNITE garantit que toutes les opérations de comparaison entre les valeurs de l'horloge interne d'une unité d'horodatage et du temps de référence et les opérations de synchronisation de l'horloge interne seront tracées pour être consultées par un auditeur.

OSP.POLITIQUE_HORODATAGE_DEFAUT

Cette OSP est couverte par O.POLITIQUE_HORODATAGE_DEFAUT.

OSP.GESTION_CONTEXTE

Cette OSP est couverte par O.CREATION_CONTEXTE_NON_OPERATIONNEL qui garantit que des contextes d'horodatage non opérationnels peuvent être créés par un administrateur de sécurité, par O.CONSULT_CONTEXTE qui assure que les informations contenues dans les contextes d'horodatage (à l'exception de la clé privée du contexte) sont consultables par un administrateur de sécurité, et par O.ARRET_CONTEXTE qui garantit que les contextes d'horodatage peuvent être définitivement arrêtés.

OSP.IMPORT_CERTIFICAT

Cette OSP est couverte par O.IMPORT_CERTIFICAT.

OSP.PROTOCOLE_REQUETE

Cette OSP est couverte par O.PROTOCOLE_REQUETE.

4.3.3. Hypothèses

4.3.3.1. Hypothèses sur l'usage attendu de la TOE

A.VERIF_JETON

Cette hypothèse est supportée par OE.VERIF_JETON.

A.ADMIN

Cette hypothèse est supportée par OE.ADMIN qui impose la formation des administrateurs pour les tâches dont ils ont la responsabilité.

A.AUDIT

Cette hypothèse est supportée par OE.ANALYSE_AUDIT qui impose l'analyse régulière des évènements d'audit par l'auditeur.

4.3.3.2. Hypothèses sur l'environnement d'utilisation de la TOE

A.AUTORITE_CERT

Cette hypothèse est supportée par OE.AUTORITE_CERT. OE.IMPORT_CERTIFICAT supporte également cette hypothèse car il impose de vérifier, lors de l'import du certificat d'unité d'horodatage, que celui-ci provient bien d'une Autorité de Certification habilitée à délivrer des certificats pour un contexte donné.

A.AUTORITE_HORODATAGE

Cette hypothèse est supportée par OE.AUTORITE_HORODATAGE. OE.DEMANDE_CERTIFICAT supporte également cette hypothèse car il impose la vérification d'informations contenues dans le contexte non opérationnel lors de la demande de certificat auprès d'une Autorité de Certification.

A.TEMPS_REFERENCE

Cette hypothèse est supportée par OE.TEMPS_REFERENCE.

A.LOCAL

Cette hypothèse est supportée par OE.PROTECTION_PHYSIQUE et OE.RESEAU qui imposent que les équipements constituant la TOE se trouvent dans un lieu sécurisé et soient connectés sur un réseau qui garantit que les services et les biens sensibles de la TOE ne seront pas compromis.

A.LOCAL_ADMIN

Cette hypothèse est supportée par OE.LOCAL_ADMIN qui impose que l'administration de la TOE s'effectue localement depuis l'environnement sécurisé à accès contrôlé dans lequel se trouvent les équipements constituant la TOE.

A.RESEAU

Cette hypothèse est supportée par OE.RESEAU qui impose que les équipements constituant la TOE soient connectés sur un réseau qui garantit que les services et les biens sensibles de la TOE ne seront pas compromis.

A.SUPERVISION

Cette hypothèse est supportée par OE.SUPERVISION qui assure que l'état opérationnel de l'unité d'horodatage puisse être consulté à distance par un superviseur.

5. EXIGENCES DE SÉCURITÉ EXPLICITES

Toutes les exigences de sécurité présentes dans cette cible sont extraites des parties 2 et 3 des Critères Communs [CC].

22, avenue Galilée – 92350 Le Plessis Robinson – France – Tél. : +33 (0)1 41 28 40 00 – Fax : +33 (0)1 41 28 40 40

6. EXIGENCES DE SÉCURITÉ

6.1. EXIGENCES FONCTIONNELLES POUR LA TOE

Le texte extrait des Critères Communs est en caractères normaux. Les affectations (« assignements ») et les sélections (« selections ») sont en caractères **gras**. Les raffinements (« refinements ») sont en caractères *italiques*. Les itérations sont identifiées par le signe « / » pour différencier les exigences ; comme par exemple pour FAU_ARP.1/Security_Alarm.

Ci-dessous la liste des sujets, objets, opérations et leurs attributs de sécurité utilisés dans la formulation des exigences de sécurité fonctionnelles:

Context Management Policy

- **Subjects:** subject representing the Security Administrator (S.security_admin),
- **Operations:** creation, modification, destruction and consultation of the timestamping contexts (OP.context_creation, OP.context_modification, OP.context_destruction, and OP.context_consultation respectively),
- **Objects:** timestamping contexts (OB.timestamping_context),
- **Security attributes:**
  - the security attribute AT.context_operational associated with a timestamping context (OB.timestamping_context),
  - the security attributes AT.non_operational_context_complete and AT.non_operational_context_created associated with a timestamping context (OB.timestamping_context),

Key Management Policy

- **Subjects:** subjects that export the public key generated by the TOE and import the corresponding public key certificate of the timestamping unit into the TOE to create an operational context (S.public_key_export_module and S.timestamping_unit_certificate_import_module respectively),
- **Operations:**
  - export of the public key to obtain the timestamping unit certificate (OP.public_key_export),
  - import of the timestamping unit certificate (OP.timestamping_unit_certificate_import),
- **Information:**
  - value of the timestamping unit certificate imported into the TOE (I.imported_certificate),
  - value of the public key contained in the timestamping unit certificate imported into the TOE (I.imported_certificate_public_key),
  - value of the public key of the non operational context into which the certificate is imported (I.non_operational_context_public_key),
  - value of the private key of the non operational context into which the certificate is imported (I.non_operational_context_private_key),
  - value of the private key validity period contained in the timestamping unit certificate imported into the TOE, if present (I.imported_certificate_private_key_validity_period),
  - value of the public key algorithm identifier (I.public_key_algorithm_identifier),
- **Objects:** timestamping contexts (OB.timestamping_context),
- **Security attributes:**
  - the security attributes AT.non_operational_context_complete and AT.non_operational_context_created associated with a non operational context (OB.timestamping_context with security attribute AT.context_operational being "False") that indicate respectively if the non operational context is complete (i.e., all required information are specified) and if the non operational context has been created by the Security Administrator,

- the security attribute AT.context_operational that indicates that a timestamping context (OB.timestamping_context) is operational following the authorized import of the timestamping unit certificate,
- the security attributes AT.private_key_initial_validity_period associated with a non operational context (OB.timestamping_context with security attribute AT.context_operational being "False") and AT.private_key_effective_validity_period associated with an operational context (OB.timestamping_context with security attribute AT.context_operational being "True") that concern the validity period of the private key of the timestamping context.

Timestamp Token Generation Policy

- **Subjects:** subjects that import timestamp token requests and exports signed timestamp tokens as responses to such requests (S.timestamp_token_request_import_module and S.timestamp_token_export_module respectively),
- **Operations:** import of timestamp token requests (OP.timestamp_token_request_import), and export of signed timestamp tokens (OP.timestamp_token_export),
- **Information:**
  - value of the imported timestamp token request (I.timestamp_token_request),
  - value of the hash algorithm identifier used to generate the data imprint contained in the imported timestamp token request (I.hash_algorithm_identifier),
  - value of the data imprint contained in the imported timestamp token request (I.data_imprint),
  - value of the timestamping policy identifier contained in the imported timestamp token request, if present (I.request_policy_identifier),
  - value of the nonce contained in the imported timestamp token request, if present (I.request_nonce),
  - value of the time contained in the exported timestamp token (I.timestamp_token_time),
  - value of the timestamping unit certificate reference (I.timestamping_unit_certificate_reference)
  - value of the used timestamping policy contained in the exported timestamp token (I.used_timestamping_policy_identifier),
  - value of the timestamp token signature (I.timestamp_token_signature),
- **Objects:** timestamp tokens (OB.timestamp_token)
- **Security attributes:**
  - the security attribute AT.context_operational associated with a timestamping context (OB.timestamping_context) that indicates that timestamp tokens can be generated using the information specified in this context,
  - the security attribute AT.internal_clock_synchronized associated with a timestamping context (OB.timestamping_context) that indicates if the internal clock is synchronized with UTC with the accuracy specified in the operational context,
  - the global security attribute AT.default_timestamping_policy_defined that indicates if a default timestamping policy has been defined by an authenticated Security Administrator.

Timestamp Token Generation Policy

- **Subjects:** subject that generates signed timestamp tokens (S.timestamp_token_generation_module),
- **Objects:** operational contexts (OB.timestamping_context with security attribute AT.context_operational being "True") generating timestamp tokens signed against the context signature private key, and generated timestamp tokens (OB.timestamp_token) containing the information present in the corresponding timestamp token requests (I.timestamp_token_request), the time value provided by the used internal clock (I.timestamp_token_time), the value of the timestamping unit certificate reference (I.timestamping_unit_certificate_reference) and the value of the used timestamping policy (I.used_timestamping_policy_identifier),
- **Operations:** creation and signature of timestamp tokens (OP.timestamp_token_creation and OP.timestamp_token_signature respectively),

- **Security attributes:**
- the security attribute AT.context_operational that indicates if the timestamping context (OB.timestamping_context) whose information are used to generate the timestamp token is operational,
- the security attribute AT.private_key_effective_validity_period associated with the used operational context (OB.timestamping_context with security attribute AT.context_operational being "True") that indicates the validity period of the context private key,
- the security attribute AT.monotonic_timestamp_token_time associated with the used operational context (OB.timestamping_context) that indicates if the time value provided by the used internal clock for the current timestamp token is greater than the time value placed in the previous timestamp token generated by this timestamping context,
- the security attribute AT.internal_clock_synchronized associated with the used operational context (OB.timestamping_context with security attribute AT.context_operational being "True") that indicates if the internal clock is synchronized with UTC with the accuracy specified in the operational context,
- the global security attribute AT.default_timestamping_policy_defined that indicates if a default timestamping policy has been defined for the timestamping system using a policy identifier by an authenticated Security Administrator.

6.1.1. Politique de gestion des contextes d'horodatage

FDP_ACC.1/Context_Management_Policy: Subset access control

FDP_ACC.1.1/Context_Management_Policy: The TSF shall enforce the **context management policy** on

- **Subjects: subject representing the Security Administrator (S.security_admin),**
- **Objects: timestamping contexts (OB.timestamping_context),**
- **Operations: creation, modification, destruction and consultation of the timestamping contexts (OP.context_creation, OP.context_modification, OP.context_destruction, and OP.context_consultation respectively)**.

FDP_ACF.1/Context_Management_Policy: Security attribute based access control

FDP_ACF.1.1/Context_Management_Policy The TSF shall enforce the **context management policy** to objects based on the following:

- **the security attribute AT.context_operational associated with a timestamping context (OB.timestamping_context),**
- **the security attributes AT.non_operational_context_complete and AT.non_operational_context_created associated with a timestamping context (OB.timestamping_context)**.

FDP_ACF.1.2/Context_Management_Policy The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- **The creation of a non operational context (OP.context_creation) is authorized to be performed only by an authenticated Security Administrator (S.security_admin) only if the**

following required information have been defined for this context (i.e., the value of the security attribute AT.non_operational_context_complete is "True"):

- **identification of the internal clock that shall be used to obtain the time value contained in timestamp tokens,**
- **the accuracy with UTC time that is guaranteed for the time contained in timestamping tokens,**
- **the private key validity period defined during the context creation phase,**
- **reference(s) of accepted timestamping policies,**
- **identifier(s) of authorized hash algorithms for each timestamping policy (recommendations for the choice of hash algorithms are provided in [CRYPTO-STD]).**

- **The consultation of the following information only that are contained in both non operational and operational contexts (OP.context_consultation) is authorized to be performed only by an authenticated Security Administrator (S.security_admin):**
  - **identification of the internal clock that shall be used to obtain the time value contained in timestamp tokens,**
  - **the accuracy with UTC time that is guaranteed for the time contained in timestamping tokens,**
  - **the private key validity period defined during the context creation phase,**
  - **reference(s) of the accepted timestamping policies,**
  - **identifiers of authorized hash algorithms for each timestamping policy,**
  - **the private key effective validity period (for operational contexts only),**
  - **the timestamping unit certificate (for operational contexts only).**
- **The modification of all information contained in a non operational context except the key pair value (OP.context_modification) is authorized to be performed only by an authenticated Security Administrator (S.security_admin) only if the non operational context has not yet been created (i.e., the value of the security attribute AT.non_operational_context_created associated with the non operation context is "False").**
- **The destruction of both non operational and operational contexts (OP.context_destruction) is authorized to be performed by an authenticated Security Administrator (S.security_admin)**.

FDP_ACF.1.3/Context_Management_Policy The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

- **if all the rules stated in FDP_ADF.1.4 are satisfied**.

FDP_ACF.1.4/Context_Management_Policy The TSF shall explicitly deny access of subjects to objects based on the **following rules:**

- **the modification of key pairs contained in non operational contexts (i.e., timestamping contexts for which the value of the associated security attribute AT.context_operational is "False") is not authorized,**
- **the modification of information contained in operational contexts (i.e., timestamping contexts for which the value of the associated security attribute AT.context_operational is "True") is not authorized**.

FMT_MSA.3/Context: Static attribute initialisation

FMT_MSA.3.1/Context The TSF shall enforce the **following policies:**

- **context management policy,**
- **key management policy,**
- **timestamp token generation policy,** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/Context The TSF shall allow the **following role: none** to specify alternative initial values to override the default values when an object or information is created.

Raffinement:

The security attributes concerned by these requirements are:

- the security attribute AT.non_operational_context_complete that indicates that all required information are specified for the associated non operational context (OB.timestamping_context with security attribute AT.context_operational being "False"),
- the security attribute AT.non_operational_context_created that indicates that a non operational context (OB.timestamping_context with security attribute AT.context_operational being "False") is created,
- the security attribute AT.context_operational that indicates that the context it is associated with (OB.timestamping_context) is operational,
- the security attribute AT.monotonic_timestamp_token_time associated with a timestamping context (OB.timestamping_context) that indicates if the time value provided by the internal clock for the current timestamp token is greater than the time value placed in the previous timestamp token generated by this timestamping context.

FMT_MSA.1/Context: Management of security attributes

FMT_MSA.1.1/Context The TSF shall enforce the **following policies:**

- **context management policy,**
- **key management policy,**
- **timestamp token generation policy,**

to restrict the ability to:

- **modify and query** the security attributes **AT.non_operational_context_complete, AT.non_operational_context_created and AT.context_operational** to **the Security Administrator**,
- **modify** the security attribute **AT.monotonic_timestamp_token_time** to **no role** (this security attribute is directly modified by the TOE).

Raffinement:

The modification operation on the following security attributes:

- AT.non_operational_context_complete,
- AT.context_operational,

are performed indirectly by the Security Administrator, since these attribute modifications result from operations performed by the Security Administrator (context creation and certificate import).

The Security Administrator can only specify that a non operational context is created (i.e., the Security Administrator can only modify the security attribute AT.non_operational_context_created from the "False" to the "True" value only).

The value of the security attribute AT.monotonic_timestamp_token_time is set to the "True" value by the TOE to enable the first timestamp token to be generated by an operational context.

Raffinement:

The security attribute AT.non_operational_context_created indicates that all required information of a non operational context have been specified and that the corresponding context has been created (i.e., validated) by the Security Administrator.

FMT_SMF.1/Context: Specification of Management Functions

FMT_SMF.1.1/Context The TSF shall be capable of performing the following management functions:

- **modification of the following security attributes:**
  - **AT.non_operational_context_complete,**
  - **AT.non_operational_context_created,**
  - **AT.context_operational,**
  - **AT.monotonic_timestamp_token_time,**
- **querying of the following security attributes:**
  - **AT.non_operational_context_complete,**
  - **AT.non_operational_context_created,**
  - **AT.context_operational**.

FDP_ITC.1/Context: Import of user data without security attributes

FDP_ITC.1.1/Context The TSF shall enforce the **context management policy** when importing user data, controlled under the SFP, from outside of the TOE.

Raffinement:

The imported user data correspond to the following information involved during the operations of creation and modification of timestamping contexts:

- identification of the internal clock that shall be used to obtain the time value contained in timestamp tokens,
- accuracy with UTC time that is guaranteed for the time contained in timestamping tokens,
- initial validity period of the context private key,
- reference(s) of accepted timestamping policies,
- identifier(s) of authorized hash algorithms for each timestamping policy.

FDP_ITC.1.2/Context The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3/Context The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **no additional importation control rules**.

FDP_SDI.2/Context: Stored data integrity monitoring and action

FDP_SDI.2.1/Context The TSF shall monitor user data stored in containers controlled by the TSF for **integrity errors** on all objects, based on the following attributes: **user data attributes**.

Raffinement:

The user data correpond to the timestamping contexts.

FDP_SDI.2.2/Context Upon detection of a data integrity error, the TSF shall **destroy the private key of the operational context.**

6.1.2. Politique de gestion des clés

FDP_ETC.1/Non_Operational_Context_Public_Key: Export of user data without security attributes

FDP_ETC.1.1/Non_Operational_Context_Public_Key The TSF shall enforce the **key management policy** when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.1.2/Non_Operational_Context_Public_Key The TSF shall export the user data without the user data's associated security attributes

Raffinement:

The exported user data are the public keys of non operational contexts which are generated by the TOE during the context creation phase along with the corresponding public key algorithm identifiers.

FDP_ITC.2/Timestamping_Unit_Certificate: Import of user data with security attributes

FDP_ITC.2.1/Timestamping_Unit_Certificate The TSF shall enforce the **key management policy** when importing user data, controlled under the SFP, from outside of the TOE.

Raffinement:

The imported user data are the public key certificates of timestamping units delivered by a Certification Authority.

FDP_ITC.2.2/Timestamping_Unit_Certificate The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3/Timestamping_Unit_Certificate The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4/Timestamping_Unit_Certificate The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5/Timestamping_Unit_Certificate The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **rules defined in the key management policy**.

FPT_TDC.1/Timestamping_Unit_Certificate: Inter-TSF basic TSF data consistency

FPT_TDC.1.1/Timestamping_Unit_Certificate The TSF shall provide the capability to consistently interpret **fields of the imported timestamping unit certificates** when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/Timestamping_Unit_Certificate The TSF shall use

- **the value of the public key contained in the imported certificate to verify it corresponds to the value of the non operational context public key generated during the context creation phase,**
- **the value of the private key validity period extension field of the imported certificate, if present, to derive the effective private key validity period for the context private key,** when interpreting the TSF data from another trusted IT product.

FTP_TRP.1/Timestamping_Unit_Certificate: Trusted path

FTP_TRP.1.1/Timestamping_Unit_Certificate The TSF shall provide a communication path between itself and **local** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **modification and disclosure**.

FTP_TRP.1.2/Timestamping_Unit_Certificate The TSF shall permit **local users** to initiate communication via the trusted path.

FTP_TRP.1.3/Timestamping_Unit_Certificate The TSF shall require the use of the trusted path for **initial user authentication**.

Raffinement:

Local users referred to in these requirements are the Security Administrators of the TOE who import timestamping unit certificates into the TOE.

FDP_IFC.1/Key_Management_Policy: Subset information flow control

FDP_IFC.1.1/Key_Management_Policy The TSF shall enforce the **key management policy** on**:**

- **Information:**
  - **value of the timestamping unit certificate imported into the TOE (I.imported_certificate),**
  - **value of the public key contained in the timestamping unit certificate imported into the TOE (I.imported_certificate_public_key),**
  - **value of the public key of the non operational context into which the certificate is imported (I.non_operational_context_public_key),**
  - **value of the private key of the non operational context into which the certificate is imported (I.non_operational_context_private_key),**
  - **value of the private key validity period contained in the timestamping unit certificate imported into the TOE, if present (I.imported_certificate_private_key_validity_period),**
  - **value of the public key algorithm identifier (I.public_key_algorithm_identifier),**
- **Subjects: subjects that export the public key generated by the TOE and import the corresponding public key certificate of the timestamping unit into the TOE to create an operational context (S.public_key_export_module and S.timestamping_unit_certificate_import_module respectively),**
- **Operations:**
  - **export of the public key to obtain the timestamping unit certificate (OP.public_key_export),**
  - **import of the timestamping unit certificate (OP.timestamping_unit_certificate_import),**
- **Objects: timestamping contexts (OB.timestamping_context)**.

FDP_IFF.1/Key_Management_Policy: Simple security attributes

FDP_IFF.1.1/Key_Management_Policy The TSF shall enforce the **key management policy** based on the following types of subject and information security attributes:

- **the security attributes AT.non_operational_context_complete and AT.non_operational_context_created associated with a non operational context (OB.timestamping_context with security attribute AT.context_operational being "False") that indicate respectively if the non operational context is complete (i.e., all required information are specified) and if the non operational context has been created by the Security Administrator,**
- **the security attribute AT.context_operational that indicates that a timestamping context (OB.timestamping_context) is operational following the authorized import of the timestamping unit certificate,**
- **the security attributes AT.private_key_initial_validity_period associated with a non operational context (OB.timestamping_context with security attribute AT.context_operational being "False") and AT.private_key_effective_validity_period associated with an operational context (OB.timestamping_context with security attribute AT.context_operational being "True") that concern the validity period of the private key of the timestamping context,**

- **no other security attributes.**

FDP_IFF.1.2/Key_Management_Policy The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

- **the operation OP.public_key_export enables the export of the public key of a non operational context and the identifier of the public key algorithm (I.non_operational_context_public_key and I.public_key_algorithm_identifier) from the non operational context (OB.timestamping_context with security attribute being "False") by the subject that exports the public key (S.public_key_export_module). This operation is authorized to be performed only on behalf of an authenticated Security Administrator,**
- **the operation OP.timestamping_unit_certificate_import enables the import of the certificate corresponding to the exported public key (I.timestamping_unit_certificate) into the non operational context (OB.timestamping_context with security attribute AT.context_operational being "False") by the subject that imports the certificate (S.timestamping_unit_certificate_import_module) in order to create the corresponding operational context (OB.timestamping_context with security attribute AT.context_operational being "True"). This operation is authorized to be performed only on behalf of an authenticated Security Administrator only if the following conditions hold:**
  - **the non operational context is both complete and created (the value of the security attributes AT.non_operational_context_complete and AT.non_operational_context_created are both "True"),**
  - **the value of the public key of the imported certificate (I.imported_certificate_public_key) corresponds to the value of the public key of the non operational context into which the timestamping certificate is imported (I.non_operational_context_public_key)**.

FDP_IFF.1.3/Key_Management_Policy The TSF shall enforce the **no additional information flow control SFP rules**.

FDP_IFF.1.4/Key_Management_Policy The TSF shall explicitly authorise an information flow based on the following rules:

- **derivation of the effective private key validity period (AT.private_key_effective_validity_period) associated with the private key of a non operational context. The derivation is based on the following rules:**
  - **If the imported certificate contains a private key validity period extension field, the value of the private key validity period defined during the context creation phase (AT.private_key_initial_validity_period) by an authenticated Security Administrator is ignored and the value contained in the imported certificate is considered as the effective private key validity period.**
  - **If the imported certificate does not contain a private key validity period extension field, the value of the private key validity period defined during the context creation phase by an authenticated Security Administrator is considered as the effective private key validity period.**
- **destruction of the private key of a non operational context if the associated private key validity period specified during the context creation phase (AT.private_key_initial_validity_period) has expired.**
- **destruction of the private key of an operational context if the associated effective private key validity period (AT.private_key_effective_validity_period) has expired**.

FDP_IFF.1.5/Key_Management_Policy The TSF shall explicitly deny an information flow based on the following rules:

- **private keys (I.non_operational_context_private_key) generated by the TOE shall never be exported outside the TOE,**
- **private keys (I.non_operational_context_private_key) and key pairs (I.non_operational_context_private_key and I.non_operational_context_public_key) generated outside the TOE shall never be imported into the TOE,**
- **timestamping certificates (I.imported_certificate) shall not be imported into an operational context (OB.timestamping_context with security attribute AT.context_operational being "True")**.

Raffinement:

La TOE devra fournir les moyens de:

- Déduire la bonne période de validité de la clé privée (AT.private_key_effective_validity_period) associée à la clé privée d'un contexte non opérationnel.
- Détruire la clé privée d'un contexte non opérationnel si la clé privée associée qui a été créée pendant la phase de création du contexte (AT.private_key_initial_validity_period) a expiré.
- Destruction de la clé privée d'un contexte opérationnel si la période efficace de validité de la clé privée associée (AT.private_key_effective_validity_period) a expiré.

FMT_MSA.3/Private_Key_Validity_Period: Static attribute initialisation

FMT_MSA.3.1/Private_Key_Validity_Period The TSF shall enforce the **following policies:**

- **key management policy,**
- **timestamp token generation policy,** to provide **the private key initial validity period specified by the Security Administrator during the context creation phase and the private key effective validity period computed by the TOE during the timestamping certificate import as** default values for security attributes that are used to enforce the SFP.

Raffinement:

The derivation of the effective private key validity period by the TOE (AT.private_key_effective_validity_period) is based on the following rule:

- If the imported certificate contains a private key validity period extension field, the value of the private key validity period defined during the context creation phase (AT.private_key_initial_validity_period) by an authenticated Security Administrator is ignored and the value contained in the imported certificate is considered as the effective private key validity period.
- If the imported certificate does not contain a private key validity period extension field, the value of the private key validity period defined during the context creation phase by an authenticated Security Administrator is considered as the effective private key validity period.

FMT_MSA.3.2/Private_Key_Validity_Period The TSF shall allow the **following role: none** to specify alternative initial values to override the default values when an object or information is created.

Raffinement:

The security attributes concerned by these requirements are AT.private_key_initial_validity_period and AT.private_key_effective_validity_period.

FMT_MSA.1/Private_Key_Validity_Period: Management of security attributes

FMT_MSA.1.1/Private_Key_Validity_Period The TSF shall enforce the **following policies:**

- **key management policy,**
- **timestamp token generation policy,**

to restrict the ability to:

- **query** the security attribute **AT.private_key_initial_validity_period** and
- **query and modify** the security attribute **AT.private_key_effective_validity_period**

to **the Security Administrator**.

Raffinement:

The modification operation on the security attribute AT.private_key_effective_validity_period is performed indirectly by the Security Administrator, since this attribute modification results from an operation performed by the Security Administrator (certificate import).

FMT_SMF.1/Private_Key_Validity_Period: Specification of Management Functions

FMT_SMF.1.1/Private_Key_Validity_Period The TSF shall be capable of performing the following management functions:

- **modification of the security attribute AT.private_key_effective_validity_period,**
- **querying of the security attributes AT.private_key_initial_validity_period and AT.private_key_effective_validity_period**.

FCS_CKM.1/Context_Keys: Cryptographic key generation

FCS_CKM.1.1/Context_Keys The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **RSA** and specified cryptographic key sizes **1024, 2048 or 4096** bits that meet the following: **[CRYPTO-STD]**.

Raffinement:

This requirement concerns the asymmetric key pairs used to create and verify the signature of timestamping tokens generated by a timestamping unit.

FCS_CKM.4/Context_Keys: Cryptographic key destruction

FCS_CKM.4.1/Context_Keys The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **defined in the HSM Luna PCI common criteria security target** that meets the following: **protection profile CWA 14167-2version 0.28 dated 27 october 2003 ref MCSO PP]**.

Raffinement:

This requirement concerns private keys contained in both operational and non operational contexts.

22, avenue Galilée – 92350 Le Plessis Robinson – France – Tél. : +33 (0)1 41 28 40 00 – Fax : +33 (0)1 41 28 40 40

FMT_MSA.2/Context_Keys: Secure security attributes

FMT_MSA.2.1/Context_Keys The TSF shall ensure that only secure values are accepted for **the private key validity period (AT.private_key_effective_validity_period).**

6.1.3. Politique de génération des jetons d'horodatage

FDP_ITC.1/Timestamp_Token_Request: Import of user data without security attributes

FDP_ITC.1.1/Timestamp_Token_Request The TSF shall enforce the **timestamp token generation policy** when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2/Timestamp_Token_Request The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3/Timestamp_Token_Request The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **rules defined in the timestamp token generation policy**.

FDP_ETC.1/Timestamp_Token: Export of user data without security attributes

FDP_ETC.1.1/Timestamp_Token The TSF shall enforce the **timestamp token generation policy** when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.1.2/Timestamp_Token The TSF shall export the user data without the user data's associated security attributes

Raffinement:

The exported user data are the timestamp tokens delivered by the timestamping system.

FDP_IFC.1/Timestamp_Token_Generation_Policy: Subset information flow control

FDP_IFC.1.1/Timestamp_Token_Generation_Policy The TSF shall enforce the **timestamp token generation policy** on**:**

- **Information:**
  - **value of the imported timestamp token request (I.timestamp_token_request),**
  - **value of the hash algorithm identifier used to generate the data imprint contained in the imported timestamp token request (I.hash_algorithm_identifier),**

- **value of the data imprint contained in the imported timestamp token request (I.data_imprint),**
- **value of the timestamping policy identifier contained in the imported timestamp token request, if present (I.request_policy_identifier),**
- **value of the nonce contained in the imported timestamp token request, if present (I.request_nonce),**
- **value of the time contained in the exported timestamp token (I.timestamp_token_time),**
- **value of the timestamping unit certificate reference (I.timestamping_unit_certificate_reference)**
- **value of the used timestamping policy contained in the exported timestamp token (I.used_timestamping_policy_identifier),**
- **value of the timestamp token signature (I.timestamp_token_signature).**

- **Subjects: subjects that import timestamp token requests and exports signed timestamp tokens as responses to such requests (S.timestamp_token_request_import_module and S.timestamp_token_export_module respectively).**
- **Operations: import of timestamp token requests (OP.timestamp_token_request_import), and export of signed timestamp tokens (OP.timestamp_token_export).**
- **Objects: timestamp tokens (OB.timestamp_token)**.

FDP_IFF.1/Timestamp_Token_Generation_Policy: Simple security attributes

FDP_IFF.1.1/Timestamp_Token_Generation_Policy The TSF shall enforce the **timestamp token generation policy** based on the following types of subject and information security attributes:

- **the security attribute AT.context_operational associated with a timestamping context (OB.timestamping_context) that indicates that timestamp tokens can be generated using the information specified in this context,**
- **the security attribute AT.internal_clock_synchronized associated with a timestamping context (OB.timestamping_context) that indicates if the internal clock is synchronized with UTC with the accuracy specified in the operational context,**
- **the global security attribute AT.default_timestamping_policy_defined that indicates if a default timestamping policy has been defined by an authenticated Security Administrator,**
- **no other security attributes**.

FDP_IFF.1.2/Timestamp_Token_Generation_Policy The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

- **the operation OP.timestamp_token_request_import enables the import of timestamp token requests (I.timestamp_token_request) by the subject that import timestamp token requests (S.timestamp_token_request_import_module). This operation is only authorized if the following conditions hold:**
  - **the value of the timestamping policy identifier contained in the request, if present (I.request_policy_identifier) references a timestamping policy accepted by the timestamping system (i.e., there exists at least one timestamping context whose security attribute AT.context_operational is "True" that accepts this policy) and a default timestamping policy has been defined by an authenticated Security Administrator to be used in the case a timestamping policy identifier is not specified in the request (the security attribute AT.default_timestamping_policy_defined is "True"),**

- **the value of the hash algorithm identifier contained in the request (I.hash_algorithm_identifier) is authorized by the used timestamping policy defined in the used operational context (OB.timestamping_context with security attribute AT.context_operational being "True"),**
- **the length of the data imprint contained in the request (I.data_imprint) is consistent with the hash algorithm identifier (I.hash_algorithm_identifier),**
- **the internal clock referenced in the used operational context is synchronized with UTC with the accuracy defined in the used operational context (the security attribute AT.internal_clock_synchronized is "True"),**

- **the operation OP.timestamp_token_export enables the export of signed timestamp tokens that contain all information present in the corresponding requests (I.timestamp_token_request), the value of the timestamping unit certificate reference (I.timestamping_unit_certificate_reference), the value of the used timestamping policy (I.used_timepstamping_policy_identifier), the value of the time provided by the used internal clock (I.timestamp_token_time), the value of the nonce if present in the token request (I.request_nonce) and the value of the timestamp token signature (I.timestamp_token_signature) by the subject that export timestamp tokens (S.timestamp_token_export_module). This operation is only authorized if the following conditions hold:**
  - **the internal clock referenced in the used operational context is synchronized with UTC with the accuracy defined in the used operational context (the security attribute AT.internal_clock_synchronized is "True")**.

FDP_IFF.1.3/Timestamp_Token_Generation_Policy The TSF shall enforce the **no additional information flow control SFP rules**.

FDP_IFF.1.4/Timestamp_Token_Generation_Policy The TSF shall explicitly authorise an information flow based on the following rules: **timestamp token requests that conform to the expected request format shall be imported into the TOE**.

FDP_IFF.1.5/Timestamp_Token_Generation_Policy The TSF shall explicitly deny an information flow based on the following rules: **timestamp token requests that do not conform to the expected request format shall not be imported into the TOE**.

Raffinement:

The ST author shall specify the expected timestamp request format.

FMT_MSA.3/Default_Timestamping_Policy: Static attribute initialisation

FMT_MSA.3.1/Default_Timestamping_Policy The TSF shall enforce the **timestamp token generation policy** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/Default_Timestamping_Policy The TSF shall allow the **Security Administrator** to specify alternative initial values to override the default values when an object or information is created.

Raffinement:

These requirements concern the security attribute AT.default_timestamping_policy_defined. The Security Administrator can specify an alternative value for this security attribute by specifying the reference of the default timestamping policy for the timestamping system.

FMT_MSA.3/Internal_Clock: Static attribute initialisation

FMT_MSA.3.1/Internal_Clock The TSF shall enforce the **timestamp token generation policy** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/Internal_Clock The TSF shall allow the **Security Administrator** to specify alternative initial values to override the default values when an object or information is created.

Raffinement:

These requirements concern the security attribute AT.internal_clock_synchronized. The Security Administrator can specify an alternative value for this security attribute at the time of the initial synchronization of the internal clock during the timestamping unit initialization phase.

FMT_MSA.1/Default_Timestamping_Policy: Management of security attributes

FMT_MSA.1.1/Default_Timestamping_Policy The TSF shall enforce the **timestamp token generation policy** to restrict the ability to **modify and query** the security attributes **AT.default_timestamping_policy_defined** to **the Security Administrator**.

FMT_MSA.1/Internal_Clock: Management of security attributes

FMT_MSA.1.1/Internal_Clock The TSF shall enforce the **timestamp token generation policy** to restrict the ability to **query and modify** the security attributes **AT.internal_clock_synchronized** to **the Security Administrator (and the TOE for the modification operation)**.

FDP_ACC.1/Timestamp_Token_Generation_Policy: Subset access control

FDP_ACC.1.1/Timestamp_Token_Generation_Policy The TSF shall enforce the **timestamp token generation policy** on

- **Objects: operational contexts (OB.timestamping_context with security attribute AT.context_operational being "True") generating timestamp tokens signed against the context signature private key, and generated timestamp tokens (OB.timestamp_token) containing the information present in the corresponding timestamp token requests (I.timestamp_token_request), the time value provided by the used internal clock (I.timestamp_token_time), the value of the timestamping unit certificate reference (I.timestamping_unit_certificate_reference) and the value of the used timestamping policy (I.used_timestamping_policy_identifier),**
- **Subjects: subject that generates signed timestamp tokens (S.timestamp_token_generation_module),**
- **Operations: creation and signature of timestamp tokens (OP.timestamp_token_creation and OP.timestamp_token_signature respectively)**.

FDP_ACF.1/Timestamp_Token_Generation_Policy: Security attribute based access control

FDP_ACF.1.1/Timestamp_Token_Generation_Policy The TSF shall enforce the **timestamp token generation policy** to objects based on the following:

- **the security attribute AT.context_operational that indicates if the timestamping context (OB.timestamping_context) whose information are used to generate the timestamp token is operational,**
- **the security attribute AT.private_key_effective_validity_period associated with the used operational context (OB.timestamping_context with security attribute AT.context_operational being "True") that indicates the validity period of the context private key,**
- **the security attribute AT.monotonic_timestamp_token_time associated with the used operational context (OB.timestamping_context) that indicates if the time value provided by the used internal clock for the current timestamp token is greater than the time value placed in the previous timestamp token generated by this timestamping context,**
- **the security attribute AT.internal_clock_synchronized associated with the used operational context (OB.timestamping_context with security attribute AT.context_operational being "True") that indicates if the internal clock is synchronized with UTC with the accuracy specified in the operational context,**
- **the global security attribute AT.default_timestamping_policy_defined that indicates if a default timestamping policy has been defined for the timestamping system using a policy identifier by an authenticated Security Administrator,**
- **no other security attributes**.

FDP_ACF.1.2/Timestamp_Token_Generation_Policy The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- **the creation of timestamp tokens (OP.timestamp_token_creation on OB.timestamp_token) is authorized to be performed only by the subject that generates timestamp tokens (S.timestamp_token_generation_module) only if the following conditions hold:**
  - **the context whose information are used to generate the timestamp token is operational (the security attribute AT.context_operational associated with OB.timestamping_context is "True"),**
  - **the time value provided by the internal clock of the used timestamping context is greater than the time value placed in the previous timestamp token generated by this context (the security attribute AT.monotonic_timestamp_token_time is "True"),**
  - **the context whose information are used to generate the timestamp token supports the timestamping policy specified in the token request or the default timestamping policy when no timestamping policy has been specified in the token request (the global security attribute AT.default_timestamping_policy_defined is "True"),**
  - **the used internal clock is synchronized with UTC with the accuracy defined in the used operational context (the security attribute AT.internal_clock_synchronized is "True"),**
- **the signature of timestamp tokens (OP.timestamp_token_signature on OB.timestamp_token) is authorized to be performed by the subject that generates timestamp tokens (S.timestamp_token_generation_module) only if the following conditions hold:**
  - **the context whose information are used to generate the timestamp token is operational (the security attribute AT.context_operational associated with OB.timestamping_context is "True"),**

- **the context private key used to generate the signature of the timestamp token is valid (the date and time of the signature generation is included in the private key validity period defined by the security attribute AT.private_key_effective_validity_period associated with the operational context),**
- **the internal clock is synchronized with UTC with the accuracy defined in the used operational context (the security attribute AT.internal_clock_synchronized is "True")**.

FDP_ACF.1.3/Timestamp_Token_Generation_Policy The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

- **if all the rules stated in FDP_ACF.1.2 are satisfied**.

FDP_ACF.1.4/Timestamp_Token_Generation_Policy The TSF shall explicitly deny access of subjects to objects based on the

- **if one of the rules stated in FDP_ACF.1.2 is not satisfied**.

FCS_COP.1/Timestamp_Token: Cryptographic operation

FCS_COP.1.1/Timestamp_Token The TSF shall perform **asymmetric signature generation** in accordance with a specified cryptographic algorithm **SHA1 with RSA or SHA256 with RSA** and cryptographic key sizes **1024, 2048 or 4096 bits** that meet the following: **[CRYPTO-STD]**.

Raffinement:

This operation is used to generate digital signatures on the timestamp tokens delivered by the TOE.

Note d'application

Lorsque l'algorithme de génération de signature utilisé est de type signature numérique avec appendice, la génération de signature du jeton d'horodatage inclut un algorithme asymétrique de signature et également un algorithme de hachage.

FMT_SMF.1/Default_Timestamping_Policy: Specification of Management Functions

FMT_SMF.1.1/Default_Timestamping_Policy The TSF shall be capable of performing the following management functions:

- **Definition by an authenticated Security Administrator using a timestamping policy identifier of the default timestamping policy to be applied by the timestamping system when no timestamping policy is specified in the timestamp token request,**
- **Definition by an authenticated Security Administrator using hash algorithm identifiers of the authorized hash algorithms accepted for the default timestamping policy,**
- **Modification and querying of the security attribute AT.default_timestamping_policy_defined**.

FDP_ITC.1/Default_Timestamping_Policy: Import of user data without security attributes

FDP_ITC.1.1/Default_Timestamping_Policy The TSF shall enforce the **timestamp token generation policy** when importing user data, controlled under the SFP, from outside of the TOE.

Raffinement:

The imported user data correspond to the reference of the default timestamping policy defined by the Security Administrator.

FDP_ITC.1.2/Default_Timestamping_Policy The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3/Default_Timestamping_Policy The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **no additional importation control rules**.

FMT_SMF.1/Internal_Clock: Specification of Management Functions

FMT_SMF.1.1/Internal_Clock The TSF shall be capable of performing the following management functions:

- **query the security attribute AT.internal_clock_synchronized,**
- **set the security attribute AT.internal_clock_synchronized to "Synchronized" if the internal clock is synchronized with UTC with the accuracy defined in the used operational context (function identified by OP.set_to_synchronized),**
- **set the security attribute AT.internal_clock_synchronized to "Not synchronized" if the internal clock is not synchronized with UTC with the accuracy defined in the used operational context (function identified by OP.set_to_not_synchronized),**
- **synchronize the internal clock of a timestamping unit (function identified by OP.synchronize),**
- **periodically compare the time difference between the internal clock of a timestamping unit and the time reference with an authorized value: if the time difference is greater than the authorized value then OP.set_to_not_synchronized is performed, otherwise OP.set_to_synchronized is performed,**
- **periodically record the time difference between the internal clock of a timestamping unit and the time reference to create and update an history of those time differences,**
- **periodically verify the synchronization of the internal clock of a timestamping unit by making use of the history of time differences between this internal clock and the time reference: if the history of the time differences is not in conformance with the drift authorized over a given time period then OP.set_to_not_synchronized is performed, otherwise OP.synchronize is performed depending on the decision made by the synchronization verification algorithm,**
- **initialize the time reference and the internal clock during the initialization phase of a timestamping unit,**
- **update the time reference: this function shall be performed right before the periodic comparison since the time reference represents a local approximation of UTC time**.

FMT_MTD.1/Internal_Clock: Management of TSF data

FMT_MTD.1.1/Internal_Clock The TSF shall restrict the ability to **initialize** the **internal clock of a timestamping unit** to **the Security Administrator**.

FDP_ITC.1/Internal_Clock: Import of user data without security attributes

FDP_ITC.1.1/Internal_Clock The TSF shall enforce the **timestamp token generation policy** when importing user data, controlled under the SFP, from outside of the TOE.

Raffinement:

The imported user data correspond to the time value used to synchronize the internal clock during the initialization phase of a timestamping unit and the information required to initialize and update the time reference.

FDP_ITC.1.2/Internal_Clock The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3/Internal_Clock The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **no additional importation control rules**.

FMT_SMF.1/Temporary_Interruption: Specification of Management Functions

FMT_SMF.1.1/Temporary_Interruption The TSF shall be capable of performing the following management functions:

- **supervision of the synchronization of the TOE,**
- **interruption of the timestamping service in the following cases:**
  - **the state of the internal clock is "Not synchronized" for the operational context used to generate timestamp tokens (i.e., the security attribute AT.internal_clock_synchronized is "False")**.

FPT_TDC.1/Hash_Algorithms: Inter-TSF basic TSF data consistency

FPT_TDC.1.1/Hash_Algorithms The TSF shall provide the capability to consistently interpret **the cryptographic hash algorithm identifiers associated with each accepted timestamping policy** when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/Hash_Algorithms The TSF shall **use Object Identifier syntax** when interpreting the TSF data from another trusted IT product.

FPT_TDC.1/Timestamping_Policies: Inter-TSF basic TSF data consistency

FPT_TDC.1.1/Timestamping_Policies The TSF shall provide the capability to consistently interpret **the timestamping policy identifiers that can be contained in timestamping token requests** when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/Timestamping_Policies The TSF shall use **use Object Identifier syntax** when interpreting the TSF data from another trusted IT product.

6.1.4. Rôles

FMT_SMR.1: Security roles

FMT_SMR.1.1 The TSF shall maintain the roles

- **Security Administrator,**
- **Auditor**.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

FIA_UID.2: User identification before any action

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.2: User authentication before any action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Raffinement:

The users referred to in this requirement are the Administrators (Security administrator and Auditor) of the TOE.

6.1.5. Protection des TSF

FPT_TST.1: TSF testing

FPT_TST.1.1 The TSF shall run a suite of self tests **at the conditions of a return to an operational state following a temporary service interruption, at the request of the authorised user and during initial start-up** to demonstrate the correct operation of **the TSF**.

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of **TSF data**.

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

Raffinement:

The authorized user referred to in these requirements is the Security Administrator of the TOE.

FPT_RCV.2: Automated recovery

FPT_RCV.2.1 When automated recovery from**:**

- **loss of synchronization for internal clocks (i.e., the security attribute AT.internal_clock_synchronized is "False"),**
- **restart after a power shutdown,**

is not possible, the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.

Raffinement:

Return to a secure state when automated recovery is not possible is authorized only to be performed by a Security Administrator.

FPT_RCV.2.2 For the **lost of synchronization for internal clocks (i.e., the security attribute AT.internal_clock_synchronized is "False")**, the TSF shall ensure the return of the TOE to a secure state using automated procedures.

6.1.6. Audit et alertes de sécurité

FAU_GEN.1/Internal_Clock: Audit data generation

FAU_GEN.1.1/Internal_Clock The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the **detailed** level of audit; and

c) **for each internal clock:**

- **last successful comparison between the internal clock and the time reference (date of comparison operation and values of internal clock and time reference),**
- **synchronizations of the internal clock (date of synchronization operation and value of synchronization correction),**
- **no other specifically defined auditable events**.

FAU_GEN.1.2/Internal_Clock The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **no other audit relevant information**.

Raffinement:

The audit events considered in these requirements concern the verifications of synchronization and the synchronizations of the timestamping unit internal clocks.

FAU_GEN.1/Administration: Audit data generation

FAU_GEN.1.1/Administration The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the **detailed** level of audit; and

c) **no other specifically defined auditable events**.

FAU_GEN.1.2/Administration The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **no other audit relevant information**.

Raffinement:

The audit events considered in these requirements concern all operations related to the administration of the TOE.

FAU_SAR.1: Audit review

FAU_SAR.1.1 The TSF shall provide **Auditors** with the capability to read **all audit information** from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.3: Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply **searches, sorting and/or ordering** of audit data based on: **date, period, audit data identifier, timestamping unit**.

FAU_STG.1: Protected audit trail storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to **prevent** unauthorised modifications to the stored audit records in the audit trail.

FAU_ARP.1/Security_Alarm: Security alarms

FAU_ARP.1.1/Security_Alarm The TSF shall take **the following actions:**

- **a security alarm is raised to the Security Administrator and to the Auditor,**

FAU_SAA.1/Security_Alarm: Potential violation analysis

FAU_SAA.1.1/Security_Alarm The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2/Security_Alarm The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of**:**

- **repeat synchronizations of the internal clock of a timestamping unit,**

b) **other rules:**

- **missing or corrupted stored data,**
- **failed to validate the timestamping certificate,**
- **failed to tore audit events,**
- **instantaneous time difference between the internal clock of a timestamping unit and the time reference greater than an authorized value,**
- **history of the time differences between the internal clock of a timestamping unit and the time reference not in conformance with the drift authorized over a given period of time,**

FPT_STM.1: Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

Raffinement:

Those reliable time stamps are provided by the TSF for its own use.

FAU_STG.4: Prevention of audit data loss

FAU_STG.4.1 The TSF shall **ignore audited events** and **a security alarm is raised to the Security Administrator and to the Auditor** if the audit trail is full.

FAU_STG.2: Guarantees of audit data availability

FAU_STG.2.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.2.2 The TSF shall be able to **prevent** unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.2.3 The TSF shall ensure that audit records stored **during the last week** will be maintained available when the following conditions occur: **attack.**

6.2. EXIGENCES D'ASSURANCE POUR LA TOE

Le niveau visé est **EAL3 augmenté** des composants ALC_FLR.3.

Tableau 1 Synthèse des exigences d'assurance

Exigences		Intitulés
ADV : Development		
	ADV_ARC.1	Security architecture description
	ADV_FSP.3	Functional specification with complete summary
	ADV_TDS.2	Architectural design
AGD : Guidance documents		
	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC : Life-cycle support		
	ALC_CMC.3	Authorisation controls
	ALC_CMS.3	Implementation representation CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_FLR.3	Systematic flaw remediation
ASE : Security Target evaluation		

	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
ATE : Tests		
	ATE_FUN.1	Functional testing
	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_IND.2	Independent testing - sample
AVA : Vulnerability assessment		
	AVA_VAN.2	Vulnerability analysis

6.3. ARGUMENTAIRE DES EXIGENCES DE SÉCURITÉ

6.3.1. Argumentaire de couverture des objectifs de sécurité

6.3.1.1. Objectifs de sécurité sur les services rendus par la TOE

O.PROTOCOLE_REQUETE

Cet objectif est couvert par la politique de génération de jetons d'horodatage (FDP_IFC.1/Timestamp_Token_Generation_Policy, FDP_IFF.1/Timestamp_Token_Generation_Policy, FMT_MSA.3/Default_Timestamping_Policy, FMT_MSA.3/Internal_Clock, FMT_MSA.3/Context, FMT_MSA.1/Default_Timestamping_Policy, FMT_MSA.1/Internal_Clock, FMT_MSA.1/Context et FMT_SMF.1/Context_Management_Policy, FMT_SMF.1/Default_Timestamping_Policy, FMT_SMF.1/Internal_Clock) qui contrôle les requêtes de jetons d'horodatage ainsi que les jetons délivrés en retour par le système d'horodatage.

Cet objectif est également couvert par FDP_ITC.1/Timestamp_Token_Request et FDP_ETC.1/Timestamp_Token qui font référence à la politique de génération de jetons d'horodatage pour l'import des requêtes et l'export des jetons respectivement. De plus, FPT_TDC.1/Hash_Algorithms et FPT_TDC.1/Timestamping_Policies couvrent cet objectif car ils garantissent l'interprétation cohérente des identifiants d'algorithmes de hachage et de politiques d'horodatage.

O.GENERATION_JETONS

Cet objectif est couvert par la politique de génération de jetons (FDP_ACC.1/Timestamp_Token_Generation_Policy, FDP_ACF.1/Timestamp_Token_Generation_Policy, FMT_MSA.3/Default_Timestamping_Policy, FMT_MSA.3/Internal_Clock, FMT_MSA.3/Context, FMT_MSA.3/Private_Key_Validity_Period, FMT_MSA.1/Default_Timestamping_Policy, FMT_MSA.1/Internal_Clock, FMT_MSA.1/Context, FMT_MSA.1/Private_Key_Validity_Period, FMT_SMF.1/Context_Management_Policy,

FMT_SMF.1/Default_Timestamping_Policy, FMT_SMF.1/Internal_Clock et FMT_SMF.1/Private_Key_Validity_Period) qui contrôle les opérations de création et de signature des jetons d'horodatage. De plus, cet objectif est également couvert par FCS_COP.1/Timestamp_Token qui fournit l'opération de cryptographie asymétrique de génération de signature numérique des jetons d'horodatage.

6.3.1.2. Objectifs de sécurité pour protéger les biens sensibles de la TOE

6.3.1.2.1. Gestion des requêtes de jetons d'horodatage

O.VERIF_REQUETE

Cet objectif est couvert par la politique de génération de jetons d'horodatage (FDP_IFC.1/Timestamp_Token_Generation_Policy, FDP_IFF.1/Timestamp_Token_Generation_Policy, FMT_MSA.3/Default_Timestamping_Policy, FMT_MSA.3/Internal_Clock, FMT_MSA.3/Context, FMT_MSA.1/Default_Timestamping_Policy, FMT_MSA.1/Internal_Clock, FMT_MSA.1/Context et FMT_SMF.1/Context_Management_Policy, FMT_SMF.1/Default_Timestamping_Policy, FMT_SMF.1/Internal_Clock) qui interdit l'import de requêtes dont le format n'est pas conforme au format attendu par le système d'horodatage. Cet objectif est également couvert par FDP_ITC.1/Timestamp_Token_Request qui fait référence à la politique de génération de jetons d'horodatage pour l'import des requêtes.

O.VERIF_HACHAGE

Cet objectif est couvert par la politique de génération de jetons d'horodatage ((FDP_IFC.1/Timestamp_Token_Generation_Policy, FDP_IFF.1/Timestamp_Token_Generation_Policy, FMT_MSA.3/Default_Timestamping_Policy, FMT_MSA.3/Internal_Clock, FMT_MSA.3/Context, FMT_MSA.1/Default_Timestamping_Policy, FMT_MSA.1/Internal_Clock, FMT_MSA.1/Context et FMT_SMF.1/Context_Management_Policy, FMT_SMF.1/Default_Timestamping_Policy, FMT_SMF.1/Internal_Clock) qui contrôle les requêtes de jetons d'horodatage en vérifiant notamment que la longueur du condensé de document à horodater est cohérente avec l'identifiant de l'algorithme de hachage référencé, et que cet algorithme est autorisé pour la politique d'horodatage utilisée. Cet objectif est également couvert par FDP_ITC.1/Timestamp_Token_Request qui fait référence à la politique de génération de jetons d'horodatage pour l'import des requêtes. De plus, FPT_TDC.1/Hash_Algorithms couvre cet objectif car il garantit l'interprétation cohérente des identifiants d'algorithmes de hachage.

O.POLITIQUE_HORODATAGE_DEFAUT

Cet objectif est couvert par FMT_SMF.1/Default_Timestamping_Policy qui permet de définir la politique d'horodatage par défaut et les algorithmes de hachage admis pour cette politique, et par FDP_ITC.1/Default_Timestamping_Policy pour l'import de la référence de cette politique d'horodatage par défaut par l'administrateur de sécurité. De plus, FPT_TDC.1/Hash_Algorithms et FPT_TDC.1/Timestamping_Policies couvrent cet objectif car ils garantissent l'interprétation cohérente des identifiants d'algorithmes de hachage et de politiques d'horodatage.

6.3.1.2.2. Gestion des contextes d'horodatage

O.CREATION_CONTEXTE_NON_OPERATIONNEL

Cet objectif est couvert par la politique de gestion des contextes d'horodatage (FDP_ACC.1/Context_Management_Policy, FDP_ACF.1/Context_Management_Policy, FMT_MSA.1/Context, FMT_MSA.3/Context, FMT_SMF.1/Context, et FDP_SDI.2/Context) qui contrôle

notamment les opérations de création et de modification des contextes d'horodatage non opérationnels. Cet objectif est également couvert par FDP_ITC.1/Context qui fait référence à la politique de gestion des contextes d'horodatage pour l'import des informations nécessaires à la création de contextes d'horodatage non opérationnels.

O.PROTECTION_CONTEXTE_OPERATIONNEL

Cet objectif est couvert par la politique de gestion des contextes d'horodatage (FDP_ACC.1/Context_Management_Policy, FDP_ACF.1/Context_Management_Policy, FMT_MSA.1/Context, FMT_MSA.3/Context, FMT_SMF.1/Context et FDP_SDI.2/Context)) qui contrôle notamment les opérations de modification et de destruction des contextes d'horodatage.

O.CONSULT_CONTEXTE

Cet objectif est couvert par la politique de gestion des contextes d'horodatage (FDP_ACC.1/Context_Management_Policy, FDP_ACF.1/Context_Management_Policy, FMT_MSA.1/Context, FMT_MSA.3/Context et FMT_SMF.1/Context_Management_Policy) qui contrôle notamment l'opération de consultation des contextes d'horodatage.

O.ARRET_CONTEXTE

Cet objectif est couvert par la politique de gestion des contextes d'horodatage (FDP_ACC.1/Context_Management_Policy, FDP_ACF.1/Context_Management_Policy, FMT_MSA.1/Context, FMT_MSA.3/Context et FMT_SMF.1/Context_Management_Policy) qui contrôle notamment l'opération de destruction des contextes d'horodatage.

6.3.1.2.3. Gestion de la synchronisation

O.HORLOGE_INTERNE

Cet objectif est couvert par FMT_MTD.1/Internal_Clock qui garantit que l'horloge interne d'une unité d'horodatage est synchronisée initialement par un Administrateur de sécurité lors de l'initialisation de l'unité d'horodatage et par FMT_SMF.1/Internal_Clock qui assure que le suivi de la dérive et le maintien de la synchronisation par rapport au temps UTC sont effectués par la TOE en fonction de la précision garantie. Cet objectif est aussi couvert par FDP_ITC.1/Internal_Clock qui fait référence à la politique de génération des jetons d'horodatage en ce qui concerne la synchronisation de l'horloge interne de l'unité d'horodatage avec UTC. FMT_MSA.1/Internal_Clock et FMT_MSA.3/Internal_Clock couvrent également cet objectif car ils limitent la possibilité de modifier l'état de synchronisation courant à un Administrateur de sécurité authentifié et à la TOE elle-même et FPT_STM.1 assure que la date associée à chaque évènement d'audit est fiable.

6.3.1.2.4. Gestion des clés cryptographiques

O.CRYPTO

Cet objectif est couvert par toutes les exigences concernant la gestion des clés cryptographiques et les opérations cryptographiques: FCS_COP.1/Timestamp_Token, FCS_CKM.1/Context_Keys, FCS_CKM.4/Context_Keys, et FMT_MSA.2/Context_Keys.

22, avenue Galilée – 92350 Le Plessis Robinson – France – Tél. : +33 (0)1 41 28 40 00 – Fax : +33 (0)1 41 28 40 40

O.IMPORT_CERTIFICAT

Cet objectif est couvert par la politique de gestion des clés (FDP_IFC.1/Key_Management_Policy, FDP_IFF.1/Key_Management_Policy, FMT_MSA.1/Private_Key_Validity_Period, FMT_MSA.1/Context, FMT_MSA.3/Private_Key_Validity_Period, FMT_MSA.3/Context, FMT_SMF.1/Private_Key_Validity_Period et FMT_SMF.1/Context_Management_Policy) qui contrôle l'export des bi-clés générées par la TOE et l'import des certificats d'unité d'horodatage.

Cet objectif est également couvert par FDP_ETC.1/Non_Operational_Context_Public_Key et FDP_ITC.2/Timestamping_Unit_Certificate qui font référence à la politique de gestion des clés pour l'export de la clé publique d'un contexte d'horodatage non opérationnel et l'import du certificat correspondant, et par FPT_TDC.1/Timestamping_Unit_Certificate qui garantit l'interprétation cohérente de certains champs du certificat, en particulier la valeur de la clé publique. De plus, FTP_TRP.1/Timestamping_Unit_Certificate impose un chemin de confiance avec l'Administrateur de sécurité lors de l'import des certificats d'unité d'horodatage.

O.EXPORT_CLES

Cet objectif est couvert par la politique de gestion des clés (FDP_IFC.1/Key_Management_Policy et FDP_IFF.1/Key_Management_Policy) qui contrôle l'export des clés privées générées par la TOE.

O.IMPORT_CLES

Cet objectif est couvert par la politique de gestion des clés (FDP_IFC.1/Key_Management_Policy et FDP_IFF.1/Key_Management_Policy) qui contrôle l'import de clés privées ou de bi-clés générées à l'extérieur la TOE.

6.3.1.2.5. Arrêt d'une unité d'horodatage

O.ARRET_TEMP

Cet objectif est couvert par FMT_SMF.1/Temporary_Interruption qui garantit la supervision des états de synchronisation et d'alimentation et assure l'arrêt des services d'horodatage en cas de perte de synchronisation de l'horloge interne et de coupure d'alimentation externe.

O.RETOUR_ETAT_SUR

Cet objectif est couvert par FPT_RCV.2 qui garantit que la TOE peut revenir dans un état opérationnel sûr suite à une perte d'alimentation externe et à une perte de synchronisation de l'horloge interne qui entraîne l'arrêt des services d'horodatage de manière automatique ou à l'aide d'un Administrateur de sécurité. De plus, cet objectif est également couvert par FPT_TST.1 qui assure que des tests doivent être effectués par la TOE suite à un arrêt temporaire des services d'horodatage.

6.3.1.2.6. Administration

O.AUTH_ADMIN

Cet objectif est couvert par FIA_UID.2 et FIA_UAU.2 qui exigent l'identification et l'authentification des Administrateurs de sécurité et des Auditeurs avant d'effectuer toute opération d'administration ou d'audit. De plus, cet objectif est également couvert par FMT_SMR.1 qui demande le maintien des différents rôles par la TOE.

6.3.1.2.7. Audit et alertes

O.AUDIT_UNITE

Cet objectif est couvert par FAU_GEN.1/Internal_Clock qui assure la génération d'évènements d'audit pour les opérations de synchronisation de l'horloge interne et par FPT_STM.1 qui assure que la date associée à chaque évènement d'audit est fiable. De plus, cet objectif est également couvert par FAU_SAR.1 et FAU_SAR.3 qui fournissent la consultation des évènements d'audit.

O.AUDIT_ADMIN

Cet objectif est couvert par FAU_GEN.1/Administration qui assure la génération d'évènements d'audit concernant les opérations d'administration et par FPT_STM.1 qui assure que la date associée à

chaque évènement d'audit est fiable. De plus, cet objectif est également couvert par FAU_SAR.1 et FAU_SAR.3 qui fournissent la consultation des évènements d'audit.

O.PROTECTION_AUDIT

Cet objectif est couvert par FAU_STG.1, FAU_STG.2 et FAU_STG.4 qui protègent en intégrité et en disponibilité les évènements d'audit.

O.ALERTES

Cet objectif est couvert par FAU_ARP.1/Security_Alarm qui exige de lever une alerte de sécurité quand une violation potentielle de sécurité est détectée et par FAU_SAA.1/Security_Alarm qui indique les règles utilisées pour détecter ces violations potentielles.

6.3.2. Dépendances entre exigences de sécurité

6.3.2.1. Dépendances des exigences de sécurité fonctionnelles

Exigences	Dépendances CC	Dépendances Satisfaites
FDP_ACC.1/Context_Management_Policy	(FDP_ACF.1)	FDP_ACF.1/Context_Management_Policy
FDP_ACF.1/Context_Management_Policy	(FDP_ACC.1) et (FMT_MSA.3)	FDP_ACC.1/Context_Management_Policy, FMT_MSA.3/Context
FMT_MSA.3/Context	(FMT_MSA.1) et (FMT_SMR.1)	FMT_MSA.1/Context, FMT_SMR.1
FMT_MSA.1/Context	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FDP_ACC.1/Context_Management_Policy, FMT_SMF.1/Context, FDP_IFC.1/Key_Management_Policy, FDP_IFC.1/Timestamp_Token_Generation_Policy, FDP_ACC.1/Timestamp_Token_Generation_Policy, FMT_SMR.1
FMT_SMF.1/Context	Pas de dépendance	
FDP_ITC.1/Context	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_MSA.3)	FDP_ACC.1/Context_Management_Policy, FMT_MSA.3/Context
FDP_SDI.2/Context	Pas de dépendance	
FDP_ETC.1/Non_Operational_Context_Public_Key	(FDP_ACC.1 ou FDP_IFC.1)	FDP_IFC.1/Key_Management_Policy

22, avenue Galilée – 92350 Le Plessis Robinson – France – Tél. : +33 (0)1 41 28 40 00 – Fax : +33 (0)1 41 28 40 40

Exigences	Dépendances CC	Dépendances Satisfaites
FDP_ITC.2/Timestamping_Unit_Certificate	(FDP_ACC.1 ou FDP_IFC.1) et (FPT_TDC.1) et (FTP_ITC.1 ou FTP_TRP.1)	FPT_TDC.1/Timestamping_Unit_Certificate, FTP_TRP.1/Timestamping_Unit_Certificate, FDP_IFC.1/Key_Management_Policy
FPT_TDC.1/Timestamping_Unit_Certificate	Pas de dépendance	
FTP_TRP.1/Timestamping_Unit_Certificate	Pas de dépendance	
FDP_IFC.1/Key_Management_Policy	(FDP_IFF.1)	FDP_IFF.1/Key_Management_Policy
FDP_IFF.1/Key_Management_Policy	(FDP_IFC.1) et (FMT_MSA.3)	FMT_MSA.3/Context, FDP_IFC.1/Key_Management_Policy, FMT_MSA.3/Private_Key_Validity_Period
FMT_MSA.3/Private_Key_Validity_Period	(FMT_MSA.1) et (FMT_SMR.1)	FMT_MSA.1/Private_Key_Validity_Period, FMT_SMR.1
FMT_MSA.1/Private_Key_Validity_Period	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FDP_IFC.1/Key_Management_Policy, FMT_SMF.1/Private_Key_Validity_Period, FDP_IFC.1/Timestamp_Token_Generation_Policy, FDP_ACC.1/Timestamp_Token_Generation_Policy, FMT_SMR.1
FMT_SMF.1/Private_Key_Validity_Period	Pas de dépendance	
FCS_CKM.1/Context_Keys	(FCS_CKM.2 ou FCS_COP.1) et (FCS_CKM.4)	FCS_CKM.4/Context_Keys, FCS_COP.1/Timestamp_Token
FCS_CKM.4/Context_Keys	(FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2)	FCS_CKM.1/Context_Keys
FMT_MSA.2/Context_Keys	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_MSA.1) et (FMT_SMR.1)	FDP_IFC.1/Key_Management_Policy, FMT_MSA.1/Private_Key_Validity_Period, FMT_SMR.1
FDP_ITC.1/Timestamp_Token_Request	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_MSA.3)	FDP_IFC.1/Timestamp_Token_Generation_Policy, FMT_MSA.3/Internal_Clock

Exigences	Dépendances CC	Dépendances Satisfaites
FDP_ETC.1/Timestamp_Token	(FDP_ACC.1 ou FDP_IFC.1)	FDP_IFC.1/Timestamp_Token_Generation_Policy
FDP_IFC.1/Timestamp_Token_Generation_Policy	(FDP_IFF.1)	FDP_IFF.1/Timestamp_Token_Generation_Policy
FDP_IFF.1/Timestamp_Token_Generation_Policy	(FDP_IFC.1) et (FMT_MSA.3)	FMT_MSA.3/Context, FDP_IFC.1/Timestamp_Token_Generation_Policy, FMT_MSA.3/Default_Timestamping_Policy, FMT_MSA.3/Internal_Clock
FMT_MSA.3/Default_Timestamping_Policy	(FMT_MSA.1) et (FMT_SMR.1)	FMT_MSA.1/Default_Timestamping_Policy, FMT_SMR.1
FMT_MSA.3/Internal_Clock	(FMT_MSA.1) et (FMT_SMR.1)	FMT_MSA.1/Internal_Clock, FMT_SMR.1
FMT_MSA.1/Default_Timestamping_Policy	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FDP_IFC.1/Timestamp_Token_Generation_Policy, FDP_ACC.1/Timestamp_Token_Generation_Policy, FMT_SMF.1/Default_Timestamping_Policy, FMT_SMR.1
FMT_MSA.1/Internal_Clock	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FDP_IFC.1/Timestamp_Token_Generation_Policy, FDP_ACC.1/Timestamp_Token_Generation_Policy, FMT_SMF.1/Internal_Clock, FMT_SMR.1
FDP_ACC.1/Timestamp_Token_Generation_Policy	(FDP_ACF.1)	FDP_ACF.1/Timestamp_Token_Generation_Policy
FDP_ACF.1/Timestamp_Token_Generation_Policy	(FDP_ACC.1) et (FMT_MSA.3)	FMT_MSA.3/Context, FMT_MSA.3/Private_Key_Validity_Period, FMT_MSA.3/Default_Timestamping_Policy, FMT_MSA.3/Internal_Clock, FDP_ACC.1/Timestamp_Token_Generation_Policy
FCS_COP.1/Timestamp_Token	(FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2) et (FCS_CKM.4)	FCS_CKM.1/Context_Keys, FCS_CKM.4/Context_Keys
FMT_SMF.1/Default_Timestamping_Policy	Pas de dépendance	
FDP_ITC.1/Default_Timestamping_Policy	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_MSA.3)	FDP_IFC.1/Timestamp_Token_Generation_Policy, FMT_MSA.3/Default_Timestamping_Policy

Exigences	Dépendances CC	Dépendances Satisfaites
FMT_SMF.1/Internal_Clock	Pas de dépendance	
FMT_MTD.1/Internal_Clock	(FMT_SMF.1) et (FMT_SMR.1)	FMT_SMF.1/Internal_Clock, FMT_SMR.1
FDP_ITC.1/Internal_Clock	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_MSA.3)	FMT_MSA.3/Internal_Clock, FDP_ACC.1/Timestamp_Token_Generation_Policy
FMT_SMF.1/Temporary_Interruption	Pas de dépendance	
FPT_TDC.1/Hash_Algorithms	Pas de dépendance	
FPT_TDC.1/Timestamping_Policies	Pas de dépendance	
FMT_SMR.1	(FIA_UID.1)	FIA_UID.2
FIA_UID.2	Pas de dépendance	
FIA_UAU.2	(FIA_UID.1)	FIA_UID.2
FPT_TST.1	Pas de dépendance	
FPT_RCV.2	(AGD_OPE.1)	AGD_OPE.1
FAU_GEN.1/Internal_Clock	(FPT_STM.1)	FPT_STM.1
FAU_GEN.1/Administration	(FPT_STM.1)	FPT_STM.1
FAU_SAR.1	(FAU_GEN.1)	FAU_GEN.1/Internal_Clock, FAU_GEN.1/Administration
FAU_SAR.3	(FAU_SAR.1)	FAU_SAR.1
FAU_STG.1	(FAU_GEN.1)	FAU_GEN.1/Internal_Clock, FAU_GEN.1/Administration
FAU_ARP.1/Security_Alarm	(FAU_SAA.1)	FAU_SAA.1/Security_Alarm
FAU_SAA.1/Security_Alarm	(FAU_GEN.1)	FAU_GEN.1/Internal_Clock, FAU_GEN.1/Administration
FPT_STM.1	Pas de dépendance	
FAU_STG.4	(FAU_STG.1)	FAU_STG.1
FAU_STG.2	(FAU_GEN.1)	FAU_GEN.1/Internal_Clock, FAU_GEN.1/Administration

Tableau 2 Dépendances des exigences fonctionnelles

6.3.2.2. Dépendances des exigences de sécurité d'assurance

Exigences	Dépendances CC	Dépendances Satisfaites
ADV_ARC.1	(ADV_FSP.1) et (ADV_TDS.1)	ADV_FSP.3, ADV_TDS.2
ADV_FSP.3	(ADV_TDS.1)	ADV_TDS.2
ADV_TDS.2	(ADV_FSP.3)	ADV_FSP.3
AGD_OPE.1	(ADV_FSP.1)	ADV_FSP.3
AGD_PRE.1	Pas de dépendance	
ALC_CMC.3	(ALC_CMS.1) et (ALC_DVS.1) et (ALC_LCD.1)	ALC_CMS.3, ALC_DVS.1, ALC_LCD.1
ALC_CMS.3	Pas de dépendance	
ALC_DEL.1	Pas de dépendance	
ALC_DVS.1	Pas de dépendance	
ALC_FLR.3	Pas de dépendance	
ALC_LCD.1	Pas de dépendance	
ASE_CCL.1	(ASE_ECD.1) et (ASE_INT.1) et (ASE_REQ.1)	ASE_ECD.1, ASE_INT.1, ASE_REQ.2
ASE_ECD.1	Pas de dépendance	
ASE_INT.1	Pas de dépendance	
ASE_OBJ.2	(ASE_SPD.1)	ASE_SPD.1
ASE_REQ.2	(ASE_ECD.1) et (ASE_OBJ.2)	ASE_ECD.1, ASE_OBJ.2
ASE_SPD.1	Pas de dépendance	
ASE_TSS.1	(ADV_FSP.1) et (ASE_INT.1) et (ASE_REQ.1)	ADV_FSP.3, ASE_INT.1, ASE_REQ.2
ATE_COV.2	(ADV_FSP.2) et (ATE_FUN.1)	ADV_FSP.3, ATE_FUN.1
ATE_FUN.1	(ATE_COV.1)	ATE_COV.2
ATE_IND.2	(ADV_FSP.2) et (AGD_OPE.1) et (AGD_PRE.1) et (ATE_COV.1) et (ATE_FUN.1)	ADV_FSP.3, AGD_OPE.1, AGD_PRE.1, ATE_COV.2, ATE_FUN.1
ATE_DPT.1	(ADV_ARC.1) et (ADV_TDS.2) et (ATE_FUN.1)	ADV_ARC.1, ADV_TDS.2, ATE_FUN.1
AVA_VAN.2	(ADV_ARC.1) et (ADV_FSP.1) et (ADV_TDS.1) et (AGD_OPE.1) et (AGD_PRE.1)	ADV_ARC.1, ADV_FSP.3, ADV_TDS.2, AGD_OPE.1, AGD_PRE.1

Tableau 3 Dépendances des exigences d'assurance

7. RÉSUMÉ DES SPÉCIFICATIONS DE LA TOE

7.1. FONCTIONS DE SÉCURITÉ

7.1.1. Fonctions relatives aux opérations d'horodatage et de ré-horodatage

7.1.1.1. F.GESTION_CONTEXTES

L'initialisation d'une unité d'horodatage commence par la création d'un contexte non opérationnel.

A l'issue de cette phase, l'horloge interne est maintenue synchronisée uniquement à l'aide de son algorithme de synchronisation et les informations précédentes ne sont pas modifiables individuellement et ne peuvent être que globalement effacées. Ces informations sont utilisées pour faire une demande de certificat d'unité d'horodatage auprès d'une Autorité de Certification pour ce contexte non opérationnel.

L'arrêt définitif d'un contexte correspond généralement à la fin de validité de la clé privée de ce contexte. A la fin de sa période de validité, la clé privée du contexte est automatiquement détruite.

L'arrêt définitif de contexte peut également résulter d'une détection d'attaques sur le système d'horodatage qui doit entraîner la destruction de toutes les clés privées des différents contextes.

L'arrêt définitif d'un contexte peut enfin être réalisé sur demande de l'Administrateur de sécurité.

FDP_ACC.1/Context_Management_Policy> La TOE contrôle l'accès aux opérations de gestion des contextes d'horodatage.

FDP_ACF.1/Context_Management_Policy> La TOE contrôle l'accès aux opérations de gestion des contextes d'horodatage.

FDP_ITC.1/Context> La TOE offre une interface de configuration des contextes.

FDP_SDI.2/Context> La TOE contrôle l'intégrité des contextes gérés.

FMT_MSA.1/Context> La TOE permet la configuration du statut des contextes (opérationnels/non opérationnels).

FMT_SMF.1/Context> La TOE permet de gérer les contextes.

7.1.1.2. F.GESTION_POLITIQUE_HORODATAGE_PAR_DEFAUT

Si la requête de jeton d'horodatage ne spécifie pas de politique d'horodatage, une politique d'horodatage par défaut est utilisée. A ce titre, l'Administrateur de sécurité peut définit la politique d'horodatage par défaut sous la forme d'un identifiant de politique d'horodatage, ainsi que les algorithmes de hachage admis pour cette politique.

FDP_ITC.1/Default_Timestamping_Policy> La TOE offre une interface permettant à l'administrateur de définir la politique d'horodatage par défaut.

FMT_MSA.1/Default_Timestamping_Policy> La TOE permet la configuration de la politique d'horodatage par défaut.

FMT_MSA.2/Context_Keys> La TOE contrôle que seules des valeurs "sûres" sont acceptées pour la durée de validité des clés privées.

FMT_MSA.3/Default_Timestamping_Policy> La politique d'horodatage par défaut n'est modifiable que par l'Administrateur Sécurité.

FMT_SMF.1/Default_Timestamping_Policy> La TOE permet de gérer la politique d'horodatage par défaut.

7.1.1.3. F.HORODATAGE

La fonction principale de la TOE concerne la génération des jetons d'horodatage.

Une des interfaces de la TOE permet de recevoir des requêtes de jetons d'horodatage qui doivent contenir le condensé du document à horodater, la référence à la fonction de hachage utilisée et, de manière optionnelle, l'identifiant de la politique d'horodatage demandée et un nombre unique. Lorsque l'identifiant de la politique d'horodatage n'est pas spécifié dans la requête, une politique d'horodatage par défaut doit être utilisée. Le système traitant la requête de jeton vérifie que la fonction de hachage référencée dans la requête est bien autorisée par la politique d'horodatage utilisée, et que la longueur du condensé est adéquate pour l'algorithme en question.

Si l'unité d'horodatage supportant la politique demandée dans la requête ou la politique par défaut est créée dans le système (i.e., la référence de la politique demandée ou de la politique par défaut est présente dans le contexte d'horodatage correspondant), elle génère directement les jetons d'horodatage. Le protocole utilisé est à même d'assurer que la réponse correspond bien à la requête qui vient d'être effectuée.

FCS_COP.1/Timestamp_Token> La TOE signe les jetons d'horodatage à la demande et en cas de réactualisation des algorithmes de signature ou de hachage.

FDP_ACC.1/Timestamp_Token_Generation_Policy> La TOE applique la politique de génération des jetons d'horodatage définie à la demande ou en cas de réactualisation des algorithmes de hachage ou de signature.

FDP_ACF.1/Timestamp_Token_Generation_Policy> La TOE applique la politique de génération des jetons d'horodatage définie à la demande ou en cas de réactualisation des algorithmes de hachage ou de signature.

FDP_ETC.1/Timestamp_Token> La TOE exporte les jetons d'horodatage générés.

FDP_IFC.1/Timestamp_Token_Generation_Policy> La TOE contrôle les données fournies avec les demandes d'horodatage avant de générer un jeton.

FDP_IFF.1/Timestamp_Token_Generation_Policy> La TOE contrôle les données fournies avec les demandes d'horodatage avant de générer un jeton.

FDP_ITC.1/Timestamp_Token_Request> La TOE offre une interface permettant de recevoir des demandes d'horodatage.

FPT_TDC.1/Hash_Algorithms> La TOE permet d'identifier les algorithmes de hachage à utiliser par leur identifiant.

FPT_TDC.1/Timestamping_Policies> La TOE permet d'identifier les politiques d'horodatage à utiliser par leur identifiant.

7.1.2. Fonctions de gestion des éléments cryptographiques

7.1.2.1. F.GESTION_CLES

Il est possible d'associer un certificat de clé publique à un contexte non opérationnel. A l'issue de cette opération, le contexte devient opérationnel à condition que la clé publique figurant dans le certificat corresponde bien à la clé publique déjà présente dans le contexte. Cette opération nécessite la présence d'un Administrateur de sécurité.

En ce qui concerne la période d'utilisation effective de la clé privée :

- Soit le certificat contient une extension permettant de connaître la période d'utilisation de la clé privée. Dans ce cas, la durée d'utilisation de la clé privée qui avait été introduite pendant la phase d'initialisation est ignorée, et la valeur contenue dans l'extension est prise en compte en tant que période d'utilisation effective de la clé privée.
- Soit le certificat ne contient pas une extension permettant de connaître la période d'utilisation de la clé privée. Dans ce cas, la durée d'utilisation de la clé privée qui avait été introduite pendant la phase d'initialisation est prise en compte en tant que période d'utilisation effective de la clé privée.

FCS_CKM.1/Context_Keys> La TOE génère les biclés utilisés par chacun des contextes.

FCS_CKM.4/Context_Keys> La TOE détruit de manière sécurisée les clés privées des contextes (opérationnels ou non).

FDP_ETC.1/Non_Operational_Context_Public_Key> La TOE permet l'exportation des clés publiques des contextes gérés.

FDP_IFC.1/Key_Management_Policy> La TOE permet l'importation (e.g. importation du certificat de l'unité d'horodatage) et l'exportation (e.g. clés publiques) des données cryptographiques utiles.

22, avenue Galilée – 92350 Le Plessis Robinson – France – Tél. : +33 (0)1 41 28 40 00 – Fax : +33 (0)1 41 28 40 40

FDP_IFF.1/Key_Management_Policy> La TOE permet l'importation (e.g. importation du certificat de l'unité d'horodatage) et l'exportation (e.g. clés publiques) des données cryptographiques utiles.

FDP_ITC.2/Timestamping_Unit_Certificate> La TOE offre une interface permettant d'importer les certifcats des unités d'horodatage.

FMT_MSA.1/Private_Key_Validity_Period> La TOE permet la configuration de la durée de validité des clés privées.

FMT_MSA.3/Private_Key_Validity_Period> La durée par défaut de validité des clés n'est modifiable que par l'Administrateur Sécurité.

FMT_SMF.1/Private_Key_Validity_Period> La TOE permet de gérer la durée de validité par défaut des clés.

FPT_TDC.1/Timestamping_Unit_Certificate> La TOE est capable d'importer le certificat de l'unité d'horodatage.

FTP_TRP.1/Timestamping_Unit_Certificate> L'importation des certificats des unités d'horodatage est protégée en confidentialité et en intégrité.

7.1.3. Fonctions internes

7.1.3.1. F.ARRET_TEMPORAIRE

Les évènements suivants entraînent l'arrêt temporaire automatique d'une unité d'horodatage :

- coupure de courant,
- écart instantané entre l'horloge interne de l'unité d'horodatage et le temps de référence supérieur à une valeur autorisée,
- historique des écarts entre l'horloge interne de l'unité d'horodatage et le temps de référence non conforme à la dérive autorisée sur une période de temps donnée.

En outre, il est également possible d'arrêter temporairement une unité d'horodatage durant sa vie normale. Cette opération doit pouvoir être effectuée par un Opérateur.

Le redémarrage d'une unité d'horodatage en cas de coupure de courant est automatique si toutes les conditions de synchronisation et de sécurité sont réunies lors de la reprise du secteur. Dans le cas contraire, la remise en route nécessite la présence d'un Administrateur de sécurité.

Le redémarrage d'une unité d'horodatage en cas d'arrêt automatique est possible lorsque le contexte opérationnel associé n'a pas été définitivement arrêté (suite à une détection d'attaque par exemple). Le redémarrage nécessite dans ce cas la présence d'un Administrateur de sécurité.

En outre, il doit également être possible de mettre en route ou de remettre en route une unité d'horodatage durant sa vie normale. Cette opération doit pouvoir être effectuée par un Opérateur.

FMT_MSA.3/Context> La valeur par défaut de l'état de l'alimentation n'est pas modifiable.

FMT_SMF.1/Temporary_Interruption> La TOE permet de superviser la synchronisation de l'horologe et l'état de l'alimentation. Elle permet également d'interrompre temporairement le service d'horodatage en cas de problème.

FPT_RCV.2> En cas de problème matériel (perte d'alimentation électrique ou désynchronisation de l'horologe), la TOE redémarre et ne peut retourner dans un état opérationnel que par l'administrateur sécurité.

FPT_TST.1> Une suite de tests peut être réalisée au démarrage de la TOE ainsi qu'à la demande de l'administrateur sécurité.

7.1.3.2. F.AUDIT_ALERTES

Cette fonction permet de surveiller et tracer toutes les opérations relatives à l'administration des unités d'horodatage et au maintien de la synchronisation des horloges internes avec UTC.

Des alertes de sécurité sont générées dans les cas suivants :

- détection d'attaques sur les unités d'horodatage,
- écart instantané entre l'horloge interne d'une unité d'horodatage et le temps de référence supérieur à une valeur autorisée,
- historique des écarts non conforme à la dérive autorisée sur une période de temps donnée,

- synchronisations répétées de l'horloge interne d'une unité d'horodatage,

FAU_ARP.1/Security_Alarm> Des alarmes sont générées en cas de détection d'un problème de sécurité.

FAU_GEN.1/Administration> Toutes les opérations d'administration du système sont enregistrées dans le journal.

FAU_GEN.1/Internal_Clock> Toutes les opérations relatives à l'horloge sont enregistrées dans le journal.

FAU_SAA.1/Security_Alarm> Des alarmes sont générées en cas de problème avec la synchronisation de l'horloge ou les fonctions de journalisation (saturation espace disque).

FAU_SAR.1> La TOE fournit une interface de consultation des journaux.

FAU_SAR.3> L'interface de consultation des journaux offre des fonctionnalités de recherche et de tri.

FAU_STG.1> La TOE assure la protection en intégrité des journaux.

FAU_STG.2> La TOE assure la protection en intégrité des journaux.

FAU_STG.4> Lorsque les journaux sont pleins, une alerte est généré pour l'administrateur de sécurité et l'auditeur.

7.1.3.3. F.CONTROLE_ACCES

L'accès à la TOE est contrôlé. Seuls les administrateurs de sécurité et les auditeurs identifiés et authentifiés peuvent se connecter à la TOE.

FIA_UAU.2> Les administrateurs de la TOE doivent impérativement s'authentifier pour accéder aux fonctionnalités de la TOE.

FIA_UID.2> Les administrateurs de la TOE doivent impérativement s'identifier pour accéder aux fonctionnalités de la TOE.

FMT_SMR.1> Les rôles d'Administrateur Sécurité et d'Auditeur sont gérés par la TOE.

7.1.4. Fonctions de gestion de l'horloge

7.1.4.1. F.HORLOGE

Cette fonction permet d'assurer le suivi de la dérive des horloges internes d'unité d'horodatage et leur synchronisation avec UTC.

La synchronisation de l'horloge interne d'une unité d'horodatage avec UTC repose sur :

- la synchronisation initiale de l'horloge interne lors de la phase d'initialisation de l'unité d'horodatage par rapport à une source de temps dont la précision est connue par rapport à une source UTC(k),
- le suivi de la dérive de l'horloge interne et le maintien de la synchronisation par rapport au temps de référence durant la vie normale de l'unité d'horodatage.

Le suivi de la dérive de l'horloge interne d'une unité d'horodatage par rapport au temps de référence repose sur :

- la comparaison de l'horloge interne et du temps de référence de manière à détecter les écarts instantanés importants entre ces deux valeurs,
- la vérification de la synchronisation de l'horloge interne pour son éventuelle synchronisation qui exploite l'historique des écarts entre l'horloge interne et le temps de référence de manière à détecter les variations lentes de l'écart entre ces deux valeurs.

FDP_ITC.1/Internal_Clock> La TOE offre une interface permettant de synchroniser son horologe interne.

FMT_MSA.1/Internal_Clock> La TOE permet la configuration de l'horologe interne.

FMT_MSA.3/Internal_Clock> L'heure par défaut (i.e. avant synchronisation) n'est modifiable que par l'Administrateur Sécurité.

FMT_MTD.1/Internal_Clock> Seul l'administrateur sécurité peut initialiser l'horloge interne.

FMT_SMF.1/Internal_Clock> La TOE permet de gérer l'horloge interne.

FPT_STM.1> La TOE utilise une horloge interne fiable.

7.2. ARGUMENTAIRES DES FONCTIONS DE SÉCURITÉ

Les argumentaires de couverture des exigences fonctionnelles par les fonctions de sécurité sont directement présents dans le résumé des spécifications des fonctions (§7.1).

22, avenue Galilée – 92350 Le Plessis Robinson – France – Tél. : +33 (0)1 41 28 40 00 – Fax : +33 (0)1 41 28 40 40

VERSIONS SUCCESSIVES

Vers.	*Date*	*Émetteur*	*Vérificateur*	*Approbateur*	*Motif*
1.10	01/04/2011	C. Blad S. Blonde	S. Blonde	JF Wiorek	version TOE
1.0	04/11/2008	C. Blad S. Blonde	S Blonde	JF Wiorek	Version déposée pour le dossier d'évaluation.

DIFFUSION

Motif de la diffusion.

P.Nom	*Entité*	*P.Nom*	*Entité*

ou

Ce document est mis à disposition sous forme informatique sur serveur.

Il n'est donc pas formellement diffusé sous forme papier.

En cas d'utilisation d'un exemplaire imprimé de ce document, veuillez vous assurer, en consultant le serveur approprié, que vous disposez bien de la dernière version applicable.

22, avenue Galilée – 92350 Le Plessis Robinson – France – Tél. : +33 (0)1 41 28 40 00 – Fax : +33 (0)1 41 28 40 40