Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Premier ministre

Secrétariat général
de la défense
nationale

Direction centrale de la sécurité des systèmes d'information

Profil de protection
Module de vérification de signature électronique

Date d'émission	:	17 juillet 2008
Référence	:	PP-MVSE-CCv3.1
Version	:	1.6

Profil de protection enregistré et certifié par la Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI) sous la référence DCSSI-PP-2008/06.

Table des matières

1 INTRODUCTION 7

1.1 IDENTIFICATION 7
1.2 PRESENTATION GENERALE DU PROFIL DE PROTECTION 7
1.3 DÉFINITIONS ET ACRONYMES 8
1.4 RÉFÉRENCES 8

2 DESCRIPTION DE LA CIBLE D'ÉVALUATION 9

2.1 UTILISATEURS 9
2.2 POLITIQUES DE SIGNATURE 9
2.3 CAS D'UTILISATION 10
2.4 DESCRIPTION DE LA TOE 11
2.4.1 Composant gérant l'interaction avec l'utilisateur 11
2.4.2 Composant de sélection de la politique de signature à appliquer 12
2.4.3 Lanceur d'applications de visualisation de documents 13
2.4.4 Composant de collecte et de traitement des données de validation 14
2.4.5 Composant de vérification de signatures numériques 16
2.4.6 Composant d'administration des politiques de signature 17
2.5 ENVIRONNEMENT D'UTILISATION DE LA TOE 17

3 DÉCLARATIONS DE CONFORMITÉ 19

3.1 DÉCLARATION DE CONFORMITÉ AUX CC 19
3.2 DECLARATION DE CONFORMITE A UN PAQUET 19
3.3 DÉCLARATION DE CONFORMITÉ DU PP 19
3.4 DÉCLARATION DE CONFORMITÉ AU PP 19

4 DÉFINITION DU PROBLÈME DE SÉCURITÉ 20

4.1 BIENS 20
4.1.1 Biens à protéger par la TOE (User data) 20
4.1.2 Bien sensibles de la TOE (TSF data) 21
4.2 UTILISATEURS 23
4.3 MENACES 23
4.4 POLITIQUES DE SECURITE ORGANISATIONNELLES (OSP) 23
4.4.1 Politiques relatives à l'application d'une politique de signature 23
4.4.2 Communication des attributs signés 24
4.4.3 Présentation du document au vérificateur 24
4.4.4 Conformité aux standards 24
4.4.5 Export des données de validation 25
4.4.6 Divers 25
4.5 HYPOTHÈSES 25

5 OBJECTIFS DE SÉCURITÉ 27

5.1 OBJECTIFS DE SECURITE POUR LA TOE 27
5.1.1 Objectifs généraux 27
5.1.2 Objectifs sur les règles de vérification 27
5.1.3 Objectifs relatifs à la visualisation des données signées 28
5.1.4 Objectifs relatifs au contrôle d'invariance de la sémantique du document à vérifier .. 28
5.1.5 Conformité aux standards 29
5.2 OBJECTIFS DE SECURITE POUR L'ENVIRONNEMENT OPERATIONNEL 29

6 EXIGENCES DE SÉCURITÉ 31

6.1 EXIGENCES DE SÉCURITÉ FONCTIONNELLES 31
6.1.1 Contrôles à l'import du document 33
6.1.2 Présentation du document signé 35
6.1.3 Politiques de signature 36

6.1.4 Vérification de la signature ... 36
6.1.5 Support cryptographique ... 48
6.1.6 Identification et authentification de l'utilisateur ... 48
6.2 EXIGENCES DE SÉCURITÉ D'ASSURANCE ... 49

7 ARGUMENTAIRES ... 50

7.1 OBJECTIFS DE SECURITE / PROBLEME DE SECURITE ... 50
7.1.1 Politiques de sécurité organisationnelles (OSP) ... 50
7.1.2 Hypothèses ... 51
7.1.3 Tables de couverture entre définition du problème et objectifs de sécurité ... 52
7.2 EXIGENCES DE SECURITE / OBJECTIFS DE SECURITE ... 55
7.2.1 Objectifs ... 55
7.2.2 Tables de couverture entre objectifs et exigences de sécurité ... 62
7.3 DÉPENDANCES ... 70
7.3.1 Dépendances des exigences de sécurité fonctionnelles ... 70
7.3.2 Dépendances des exigences de sécurité d'assurance ... 75
7.4 ARGUMENTAIRE POUR L'EAL ... 76
7.5 ARGUMENTAIRE POUR LES AUGMENTATIONS A L'EAL ... 76
7.5.1 ALC_FLR.3 Systematic flaw remediation ... 76
7.5.2 AVA_VAN.3 Focused vulnerability analysis ... 76

8 NOTICE ... 77

ANNEXE A GLOSSAIRE ... 78

A.1 TERMES PROPRES AUX CRITÈRES COMMUNS ... 78
A.2 TERMES PROPRES À LA SIGNATURE ÉLECTRONIQUE ... 78

ANNEXE B ACRONYMES ... 81

Table des figures

Figure 1 : La TOE dans son environnement d'utilisation 18

Table des tableaux

Tableau 1 Identification du profil de protection 7
Tableau 2 Association politiques de sécurité organisationnelles vers objectifs de sécurité..... 53
Tableau 3 Association objectifs de sécurité vers politiques de sécurité organisationnelles..... 53
Tableau 4 Association hypothèses vers objectifs de sécurité pour l'environnement opérationnel 54
Tableau 5 Association objectifs de sécurité pour l'environnement opérationnel vers hypothèses 54
Tableau 6 Association objectifs de sécurité de la TOE vers les exigences fonctionnelles 65
Tableau 7 Association exigences fonctionnelles vers objectifs de sécurité de la TOE 69
Tableau 8 Dépendances des exigences fonctionnelles..... 72
Tableau 9 Dépendances des exigences d'assurance..... 76

1 Introduction

La présente section fournit les informations générales relatives à la gestion de document nécessaires à l'enregistrement du profil de protection.

Ainsi, la section 1.1 « Identification » fournit les instructions relatives à l'étiquetage et à l'enregistrement du profil de protection (PP).

La section 1.2 « Présentation générale du profil de protection » décrit sommairement le PP, permettant ainsi à l'utilisateur potentiel de décider de l'utilité du PP.

Elle peut être utilisée indépendamment comme présentation dans les catalogues et registres de PP.

1.1 Identification

Élément	Valeur
Titre	Profil de protection – Module de vérification de signature électronique
Auteurs	Trusted Labs
Version CC	V3.1 Révision 2
Référence	PP-MVSE-CCv3.1
Numéro de version	1.6
Mots clé	Application de vérification de signature électronique, signature électronique

Tableau 1 Identification du profil de protection

1.2 Présentation générale du profil de protection

Le présent profil de protection a été élaboré sous l'égide de la Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI) afin de faciliter la certification d'applications de vérification de signature utilisables notamment dans le cadre du développement de l'administration électronique. L'élaboration de ce profil de protection permet d'exhiber l'ensemble des objectifs de sécurité communs aux promoteurs d'application de signature électronique. Ceci permet donc aux fournisseurs de produit de développer des cibles de sécurité conformes aux attentes des promoteurs d'applications et de poser ainsi les bases d'une interopérabilité sécuritaire.

Ce profil de protection est conforme aux préconisations de la DCSSI pour la qualification de produits de sécurité au niveau standard. En mettant ce profil de protection à la disposition des fournisseurs de produits, la DCSSI souhaite donc faciliter et optimiser le développement, l'utilisation et l'appréciation de la confiance des applications de vérification de signature.

Ce profil de protection définit des exigences de sécurité pour un module qui est utilisé dans le cadre d'une application de vérification de signature électronique. Il permet de répondre aux exigences de l'article 5 (Chapitre II : Des dispositifs de vérification de signature électronique) du décret 2001-272 du 30 mars 2001. Les exigences de ce décret se rapportant plus particulièrement à la vérification de signature lorsqu'elle est réalisée sous le

contrôle direct d'un être humain, il est important de noter que ce profil de protection envisage de manière équivalente la vérification de signature qu'elle soit réalisée par un système automatisé ou par un être humain.

Bien que la certification de l'application de vérification de signature ne soit pas requise pour bénéficier de la présomption de fiabilité au sens du décret n°2001-272 du 30 mars 2001, il est recommandé de recourir à une telle certification afin d'améliorer la sécurité de l'ensemble de la chaîne de signature et de disposer de preuves complémentaires en cas de contestation de la signature démontrant que le procédé de vérification de signature utilisé n'est pas fiable (c'est à dire en cas d'apport par un tiers contestataire d'une preuve contraire remettant en cause la présomption de fiabilité de la signature).

1.3 Définitions et acronymes

Les définitions des différents termes utilisés dans ce document sont données en Annexe A.

Les acronymes utilisés dans ce document sont définis en Annexe B.

1.4 Références

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 3.1, Revision 1, September 2006.

[CC2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements. Version 3.1, Revision 2, September 2007.

[CC3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements. Version 3.1, Revision 2, September 2007.

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology. Version 3.1, Revision 2, September 2007.

[QUA-STD] Processus de qualification d'un produit de sécurité – Niveau standard. Version 1.1, 18 mars 2008. N°549/SGDN/DCSSI/SDR.

[CRYPT-STD] Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse *standard*. DCSSI. http://www.ssi.gouv.fr/fr/sciences/publications.html

[AUTH-STD] Authentification - Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse *standard*. DCSSI. http://www.ssi.gouv.fr/fr/sciences/publications.html

[KEYS-STD] Gestion de clés - Règles et recommandations concernant la gestion des clés utilisées dans les mécanismes cryptographiques de niveau de robustesse *standard*. DCSSI. http://www.ssi.gouv.fr/fr/sciences/publications.html

[CWA 14169] Secure signature-creation devices "EAL 4+", CEN/WS, Mars 2004.

[CWA 14170] Security requirements for signature creation applications, CEN/WS, Mai 2004.

[CWA 14171] General guidelines for electronic signature verification, CEN/WS, Mai 2004.

[TS 101 733] Electronic signature formats, ETSI standard, version 1.5.1, 15 décembre 2003.

2 Description de la cible d'évaluation

Cette partie du profil de protection a pour but de décrire la cible d'évaluation (TOE), le type de produit qu'elle représente ainsi que les fonctionnalités générales qu'elle supporte. En outre cette partie présente la cible d'évaluation dans le cadre d'une application de vérification de signature électronique.

La cible d'évaluation (TOE) est un module logiciel ou matériel permettant la vérification de signatures électroniques.

2.1 Utilisateurs

Le module de vérification de signature électronique peut indifféremment être invoqué par un être humain ou par un système automatisé (une application appelante).

Le terme « vérificateur » utilisé dans l'article 5 du décret du 30 mars 2001 (2001-272) correspond à une personne humaine qui utilise un dispositif de vérification de signature évalué et certifié.

Dans ce profil de protection, le terme « vérificateur » englobera aussi le cas où le vérificateur est une application appelante, bien que ce cas sorte du cadre du décret. Du point de vue des exigences exprimées dans ce profil de protection, aucune différence ne sera faite entre les deux types possibles de vérificateurs.

Note d'application

D'un point de vue pratique, les développeurs pourront définir le ou les utilisateurs de leur produit comme étant :

- soit uniquement un être humain,
- soit uniquement un système automatisé,
- soit indifféremment l'un ou l'autre.

2.2 Politiques de signature

Afin de bien comprendre les différents cas d'utilisation, il convient de définir ce qu'est une politique de signature.

Selon l'ETSI, une politique de signature est un ensemble de règles pour la création ou la validation d'une signature électronique, sous lesquelles une signature électronique peut être déterminée valide.

Elle inclut des règles définissant les attributs de signature qui doivent être fournis par le signataire, ainsi que des règles relatives à l'utilisation de tiers de confiance (CA, serveurs OSCP, autorités d'horodatage, …).

Une politique de signature comprend les éléments suivants :

- L'identification d'un ou plusieurs points de confiance et des règles permettant de construire un chemin de certification entre le certificat du signataire et l'un de ces points de confiance ;
- Les moyens à mettre en œuvre pour obtenir une référence de temps destinée à positionner dans le temps la signature numérique du signataire (ex : horodatage) ;

- Les moyens à utiliser pour vérifier le statut de révocation de chaque certificat du chemin de certification par rapport à cette référence de temps ;
- Les caractéristiques que doit comporter le certificat du signataire (ex : OID de politique de certification, *QCStatements*, *key usage*, etc.) ;
- Les types d'attributs qui, outre la référence au certificat du signataire, doivent être signés conjointement avec le document (ex : référence à une politique de signature, type d'engagement, date présumée de la signature numérique, format du document, rôle présumé du signataire, lieu présumé de la signature numérique, etc.) ;
- L'ensemble des données de validation que le signataire doit fournir ;
- Les moyens à mettre en œuvre pour obtenir une référence de temps destinée à positionner dans le temps les données de validation (ex : horodatage) ;
- Les algorithmes cryptographiques (signature et hachage) à utiliser dans le cadre de la vérification de la signature numérique du document et des données de validation.

Ce profil de protection définit un ensemble de règles minimal que tout module compatible devra supporter. Pour la vérification d'une signature électronique, la TOE pourra n'exercer qu'un sous-ensemble de toutes règles possibles selon le paramétrage défini par la politique de signature appliquée.

2.3 Cas d'utilisation

Deux cas d'utilisation sont envisagés : la vérification immédiate et la vérification ultérieure.

La vérification immédiate

La vérification immédiate correspond à une première vérification de la signature électronique réalisée dans un délai aussi court que possible après la réception de la signature électronique par le vérificateur.

La TOE est utilisée afin de procéder à un contrôle de la signature électronique selon une politique de signature choisie par le vérificateur (cf. section 2.4.2) pour s'assurer que la signature électronique est valide. Durant cette opération les données de validation nécessaires à la vérification de la signature sont soit retrouvées dans la signature électronique soit collectées par d'autres moyens. Ces données de validation incluent une référence de temps permettant d'attester l'existence de la signature numérique à une date donnée. La validité des autres données de validation est notamment contrôlée vis-à-vis de cette date de référence.

La vérification ultérieure

La vérification ultérieure correspond à une vérification de la signature électronique basée sur les données de validation collectées lors de la vérification immédiate en appliquant une politique de signature choisie par le vérificateur. Cette vérification est réalisée alors que la référence de temps (ex : tampon d'horodatage) positionnant la signature numérique dans le temps est encore valide.

Note : un troisième type de vérification devrait être envisagé dans le cas où la référence de temps apposée sur la signature numérique et/ou les données de validation lors de la vérification immédiate ne sont plus valides. Ce type de vérification impliquerait un archivage et/ou une maintenance des éléments de preuve. Ce troisième cas d'utilisation n'est pas couvert par le présent profil de protection.

2.4 Description de la TOE

La TOE comporte les briques fonctionnelles suivantes :

- Composant gérant l'interaction avec les utilisateurs
- Composant de sélection de la politique de signature à appliquer
- Composant gérant l'invariance de la sémantique du document
- Lanceur d'applications de visualisation de documents
- Composant de collecte et de traitement des données de validation
- Composant de vérification de signatures numériques
- Composant d'administration des politiques de signature

2.4.1 Composant gérant l'interaction avec l'utilisateur

Deux types d'utilisateurs sont considérés :

- Le vérificateur, et
- L'administrateur sécurité de la TOE.

A noter que le rôle d'administrateur de la machine hôte est différent de celui d'administrateur de la TOE.

2.4.1.1 Interaction avec le vérificateur

La TOE comporte une interface avec le vérificateur.

Selon le type d'utilisateur défini pour la TOE, cette interface pourra être une interface homme/machine ou une interface programmatique (API), voire une conjonction les deux.

Cette interface permet les interactions suivantes :

- Sélection du document à vérifier par le vérificateur
- Sélection d'une politique de signature à appliquer
- Communication/présentation des attributs de signature au vérificateur
- Communication du statut d'exécution lorsque la vérification de signature électronique se termine
- Communication des données de validation au vérificateur

Sélection du document à vérifier par le vérificateur

La TOE offre un moyen au vérificateur lui permettant d'indiquer quel document et quelle signature électronique il souhaite vérifier.

Sélection d'une politique de signature à appliquer

La TOE offre un moyen au vérificateur lui permettant :

- d'indiquer la politique de signature de son choix (politique de signature sélectionnée), ou
- d'utiliser la politique de signature référencée dans la signature électronique.

Communication / présentation des attributs de signature au vérificateur

La TOE offre un moyen permettant au vérificateur de prendre connaissance des attributs signés présents dans la signature électronique.

Communication du statut d'exécution lorsque la vérification de signature se termine

La TOE dispose d'un moyen lui permettant de communiquer le statut d'exécution de l'opération de vérification au vérificateur.

Export des données de validation au vérificateur

La TOE dispose d'un moyen lui permettant d'exporter les données de validation utilisées lors de la vérification de la signature électronique au vérificateur.

Ceci permet au vérificateur de sauvegarder (hors TOE) ces données pour un usage ultérieur.

2.4.1.2 Interaction avec l'administrateur

Cette interface est soit une interface homme/machine soit une interface programmatique (API) permettant à l'administrateur de sécurité d'interagir avec la TOE. A noter que le rôle d'administrateur de sécurité de la TOE est distinct de celui d'administrateur de la machine hôte sur laquelle la TOE s'exécute (voir hypothèse *H.Machine_Hôte*).

Cette interface permet à l'administrateur :

- de gérer les politiques de signatures (ajout/suppression).
- de définir les applications de visualisation à lancer en fonction des formats de document supportés
- d'initialiser le paramètre de configuration permettant d'inactiver la fonction de lancement d'une application de visualisation (lorsque la TOE est destinée à être utilisée par une machine)

2.4.2 Composant de sélection de la politique de signature à appliquer

Les contrôles opérés par le module de vérification de signature électronique dépendent d'une politique de signature.

La TOE détermine la politique de signature appliqué de la manière suivante :

- Si une politique de signature a été présélectionnée par le vérificateur, alors c'est cette politique de signature qui sera appliquée, et ce, même si une politique de signature est référencée dans la signature électronique. Si la politique référencée par la signature électronique est différente de la politique de signature appliquée, la TOE en informe le vérificateur.
- Si la politique de signature n'est pas définie par l'application appelant la TOE, alors la politique de signature appliquée sera celle référencée par la signature électronique, si une telle référence est présente. La politique de signature référencée devra alors être renvoyée à l'application appelant la TOE, à charge pour cette application de vérifier qu'elle convient au contexte d'utilisation.
- Si aucune politique de signature n'a été présélectionnée et si aucune politique de signature n'est référencée dans la signature électronique, alors soit cela constitue une erreur, soit une politique de signature par défaut sera appliquée et devra alors être renvoyée à l'application appelant la TOE, à charge pour cette application de vérifier qu'elle convient au contexte d'utilisation.

2.4.2.1 Composant gérant l'invariance de la sémantique du document

Le document à signer peut contenir des champs variables ou du code actif qui dépendent de paramètres extérieurs et qui ainsi peuvent être différents selon le contexte où le document est visualisé.

Dans certains cas, le signataire a donc pu apposer sa signature sur un document électronique dont le sens varie selon le contexte où il est visualisé.

Ceci peut induire en erreur le vérificateur qui reçoit la signature. Celui-ci pourrait en effet être amené à visualiser un document sémantiquement différent de celui présenté au signataire.

Ainsi, le contenu du document à signer doit être contrôlé pour attester que sa sémantique ne dépend pas de paramètres qui lui sont extérieurs.

La TOE s'appuie sur un module extérieur pour réaliser ce test; le contrôle de la stabilité de la sémantique du document est donc en dehors du périmètre d'évaluation.

La TOE est néanmoins chargée d'informer le vérificateur :

- Lorsque le module externe décèle que la sémantique du document n'est pas stable
- Lorsque le module externe décèle que la sémantique du document est invariante
- Lorsque le module externe se déclare incapable de contrôler l'invariance de la sémantique du document.

Note d'application :

En l'absence d'application externe de contrôle de l'invariance sémantique qualifiée, il est recommandé que le produit intègre un module interne permettant ce contrôle, que ce module fasse partie de la TOE, et que le format des documents soit fixé dans la TOE, un format dont le contenu ne peut varier par construction.

Dans ce cas, le produit reste conforme aux exigences de ce PP, moyennant :

- que sa cible de sécurité prenne en compte les menaces, hypothèses, OSP, objectifs de sécurité et exigences de sécurité correspondants au module de contrôle,

- que la TOE est contrainte à ne signer que les documents du format fixé.

2.4.3 Lanceur d'applications de visualisation de documents

Pour permettre à un vérificateur humain ou à un opérateur supervisant un système automatisé de vérification de signature d'apprécier le contenu du document électronique au moment de la vérification de la signature électronique, la TOE doit permettre, sur demande du vérificateur/opérateur, le lancement d'une application de présentation correspondant au format du document à visualiser.

Pour ce faire, la TOE définit les formats de document pour lesquels elle est capable de lancer une application de visualisation. La correspondance entre ces formats et les applications de visualisation à lancer par la TOE est définie par l'administrateur de la TOE. Ces applications sont en dehors du périmètre de la TOE.

Un paramètre de configuration, initialisé par l'administrateur de sécurité de la TOE, permet de verrouiller la fonction de lancement d'une application de visualisation d'un document, par

exemple pour faciliter son intégration dans le cadre d'un processus automatique où la visualisation des documents signés par un opérateur n'est pas mise en œuvre.

Note d'application :

En l'absence d'application externe de visualisation qualifiée, il est recommandé que le produit intègre un module interne permettant de visualiser le document, et que ce module fasse partie de la TOE.

Dans ce cas, le produit reste conforme aux exigences de ce PP, moyennant que sa cible de sécurité prenne en compte les menaces, hypothèses, OSP, objectifs de sécurité et exigences de sécurité correspondants au module de visualisation.

La fonctionnalité de visualisation du document signé est requise pour tous les produits, qu'ils soient destinés à être utilisés dans un contexte automatisé (c.-à-d., par une machine) ou non (c.-à-d., par un humain). Dans le cas de l'utilisation par une machine, le produit pourra être paramétré pour que cette fonctionnalité soit inhibée.

2.4.4 Composant de collecte et de traitement des données de validation

En conformité avec la politique de signature appliquée, ce composant assure les fonctions suivantes :

- Vérification de la conformité des attributs signés
- Positionnement de la signature numérique dans le temps
- Construction d'un chemin de certification valide
- Vérification de la validité du chemin de certification

Ces fonctions sont mises en œuvre de manière itérative tant qu'un chemin de certification valide n'a pu être construit.

Vérification de la conformité des attributs signés

La TOE s'assure de la présence et de la conformité de tous les attributs signés requis par la politique de signature.

Exemples de vérifications :

- Type d'engagement est bien parmi les types d'engagement autorisés pour cette politique
- …

Positionnement de la signature numérique dans le temps

Pour pouvoir vérifier la validité du certificat du signataire ainsi que des autres données de validation et, *in fine*, vérifier la validité de la signature électronique, la TOE doit positionner la signature numérique du document dans le temps.

« Positionner la signature numérique dans le temps » signifie *« attester son existence (en tant que donnée) à une date fournie grâce à une référence de temps de confiance ».*

Il revient à la politique de signature de définir les moyens à utiliser pour positionner la signature numérique dans le temps.

Le comportement de la TOE varie selon les modes d'utilisation de la TOE :

- Dans le mode « vérification immédiate », si une « référence de temps » n'est pas déjà présente, la TOE en collecte une, conformément à la politique de signature.
- Dans le mode « vérification ultérieure », la TOE utilise la « référence de temps » apposée au moment de la vérification immédiate, si celle-ci est fournie. Elle vérifie qu'elle est conforme à la politique de signature. Si la « référence de temps » n'est pas conforme ou bien est absente, alors la signature électronique est déclarée invalide[1]. Ce PP ne traite pas de la problématique de l'archivage et donc de la pérennité dans le temps de ce premier positionnement ainsi que des données utilisées.

Vérification de la conformité du certificat

A partir de la référence du certificat du signataire figurant dans les attributs signés, la TOE doit s'assurer que le certificat qui sera utilisé comme extrémité du chemin de certification correspond bien à cette référence.

En outre, les caractéristiques de ce certificat doivent satisfaire aux exigences de la politique de signature.

Exemples:

- Contrôle que l'identifiant de politique de certification du certificat du signataire est bien inclus dans la liste définie dans la politique de signature ;
- Contrôle concernant les usages de la clé privée (*key usage*) ;
- Contrôle de la présence et de la valeur des extensions requises pour le certificat (*QCstatements*).

Construction d'un chemin de certification valide

Pour s'assurer de l'authenticité et de la validité du certificat du signataire au moment où la signature numérique a été positionnée dans le temps, la TOE recherche un chemin de certification valide entre le certificat du signataire et un point de confiance identifié dans la politique de signature.

[1] Dans certains cas, notamment si la marque de temps est un tampon d'horodatage, la marque de temps peut ne plus être valide parce que le certificat de l'autorité d'horodatage a expiré. Dans ce cas, il revient au vérificateur de prouver la validité du certificat de l'autorité d'horodatage au moment où la signature a été positionnée dans le temps.

Deux comportements sont possibles selon que la TOE s'exécute en mode « vérification immédiate » ou en mode « vérification ultérieure » :

- Vérification immédiate
  Dans ce mode, la TOE met en œuvre les fonctions requises par les règles définies dans la politique de signature jusqu'à construire un chemin de certification valide.

  Au cours de la construction du chemin, la TOE importe des données de validation (par exemple sur un réseau ou en local, ...) et contrôle qu'elles sont valides selon des règles définies dans la politique de signature appliquée.
  S'il s'avère qu'aucun chemin ne peut être construit ou que tous les chemins construits sont invalides, alors la signature électronique est déclarée invalide.
  S'il s'avère que des données ne sont pas disponibles pour attester la non révocation d'un élément du chemin, alors la vérification est déclarée incomplète et une vérification immédiate pourra être réitérée ultérieurement.
- Vérification ultérieure
  Dans le mode « vérification ultérieure », la TOE reconstruit un chemin et vérifie sa validité uniquement à partir des données collectées lors de la vérification immédiate.

  S'il s'avère qu'aucun chemin ne peut être construit avec les données disponibles ou si tous les chemins pouvant être construits avec ces mêmes données ne sont pas valides, alors la signature électronique est déclarée invalide.
  S'il manque des données pour attester la non révocation d'un élément du chemin de certification alors la signature électronique est déclarée invalide.

Selon les cas, la collecte des données de validation peut mettre en œuvre des protocoles réseau ou simplement des accès aux données en local. Les moyens utilisés pour accéder aux données (clients des protocoles réseau, pilotes de disque dur) sont considérés en dehors du périmètre de la cible d'évaluation.

La vérification de la validité d'un élément dans la chaîne de certification consiste à vérifier :

- l'intégrité et l'authenticité de l'origine de l'élément grâce à la signature numérique qui lui est associée ;
- que la date contenue dans la référence de temps apposée sur la signature numérique est incluse dans la période de validité de cet élément ;
- l'élément était non révoqué à la date contenue dans la référence de temps apposée sur la signature numérique.

Toutes ces opérations sont réalisées en conformité avec les éléments techniques définis dans la politique de signature appliquée.

Vérification de la validité du certificat

La TOE vérifie que le certificat est en cours de validité en utilisant la référence de temps apposée sur la signature numérique et la période de validité définie dans le certificat.

2.4.5 Composant de vérification de signatures numériques

Ce composant est un composant cryptographique supportant les algorithmes (hachage et vérification de signature) nécessaires à la vérification des signatures numériques impliquées dans le processus de vérification.

Les signatures numériques à vérifier sont, entre autres :

- La signature numérique du document
- Les signatures numériques contenues dans les certificats constituant la chaîne de certification
- La signature numérique du certificat racine autosigné (point de confiance).
- Les signatures numériques associées aux données de validation collectées (CRL, réponses OCSP, ARL, ...)

2.4.6 Composant d'administration des politiques de signature

Enfin, la TOE permet à un administrateur authentifié de gérer l'ensemble des politiques de signature acceptées par la TOE.

Note d'application

Les fonctions d'administration supportées par la TOE seront définies par les rédacteurs de cibles de sécurité.

Elles pourront comprendre soit aucunes, soit certaines, soit toutes les fonctions suivantes :

- l'ajout d'une politique,
- la suppression d'une politique.

2.5 Environnement d'utilisation de la TOE

Les éléments de l'environnement technique de la TOE sont les suivants :

- Le système d'exploitation de la ou des machines physiques exécutant la TOE ;
- Un dispositif logiciel et/ou matériel permettant de présenter le document au vérificateur et l'alertant si ses caractéristiques ne sont pas complètement compatibles avec les caractéristiques d'affichage requises par le document (utilisation de couleur, présence des polices nécessaires, etc. ...) ;
- Un composant logiciel et/ou matériel contrôlant l'invariance de la sémantique du document (vérifie que sa sémantique ne dépend pas de paramètres qui lui sont extérieurs).
- Les composants logiciel ou matériel fournissant les données de validation

Ces éléments sont présentés dans la figure 1.

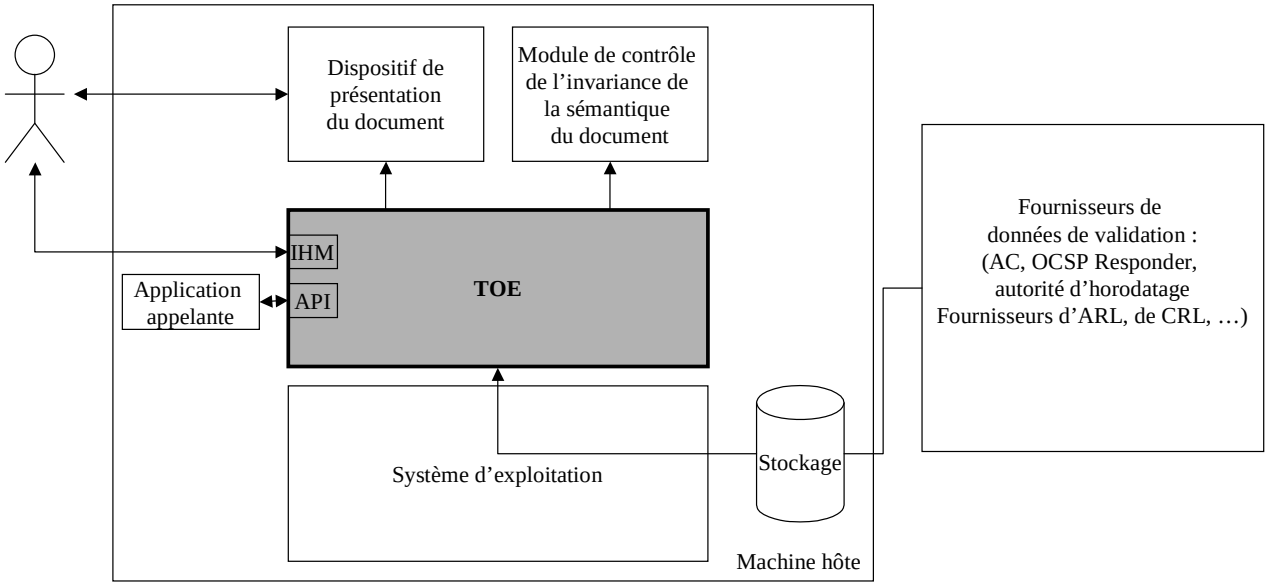

Figure 1 : La TOE dans son environnement d'utilisation

3 Déclarations de conformité

Ce chapitre contient les sections suivantes :

Déclaration de conformité aux CC (3.1)

Déclaration de conformité à un Paquet (3.2)

Déclaration de conformité du PP (3.3)

Déclaration de conformité au PP (3.4)

3.1 Déclaration de Conformité aux CC

Ce profil de protection est strictement conforme aux Critères Communs version 3.1.

Il a été écrit conformément aux:

- CC Partie 1 [CC1],
- CC Partie 2 [CC2],
- CC Partie 3 [CC3],
- et la méthodologie d'évaluation des CC [CEM].

3.2 Déclaration de conformité à un Paquet

Ce PP est conforme au paquet d'exigences d'assurance pour la qualification de niveau standard défini dans [QUA-STD].

3.3 Déclaration de conformité du PP

Ce PP ne déclare de conformité à aucun autre PP.

3.4 Déclaration de conformité au PP

La conformité retenue dans ce PP pour les Cibles de Sécurité et Profiles de Protection qui s'y déclarent conformes est la conformité **démontrable** selon la définition dans la Partie 1 des CC [CC1].

4 Définition du problème de sécurité

4.1 Biens

Cette section décrit l'ensemble des biens sous le contrôle de la TOE.

4.1.1 Biens à protéger par la TOE (User data)

4.1.1.1 Données en entrée

B.Document

Ce document est le document signé par le signataire et pour lequel la TOE doit vérifier la signature.

Il peut être fourni à la TOE soit dans le même fichier que la signature soit dans un fichier indépendant.

Protection: intégrité

B.Signature

La signature électronique d'un signataire sur le document.

Protection: intégrité

B.Attributs_Signés

Les attributs signés sont des données signées en même temps que le document. Elles fournissent au vérificateur des précisions relatives à la signature et aux circonstances dans lesquelles elle a été effectuée.

Les attributs signés comprennent:

- La référence non ambigue du certificat du signataire ou le certificat du signataire lui-même

En option:

- La politique de signature ou une référence à celle-ci
- Le type d'engagement du signataire,
- Le rôle présumé ou certifié du signataire
- La date et l'heure présumée de signature
- Le lieu présumé de signature,
- Le format du document
- etc...

Protection: intégrité

B.Données_De_Validation_En_Entrée

Les données de validation sont les données utiles à la vérification, elles peuvent comprendre:

- Le certificat du signataire,
- Des certificats d'AC, d'émetteurs de CRL, de réponses OCSP, d'unités d'horodatage,...

- Des listes de certificats révoqués (CRL)
- Des réponses OCSP
- Des listes d'autorité de certification révoquées (ARL)
- Des tampons d'horodatage

Protection: intégrité

Note d'application

Ces données peuvent être obtenues de plusieurs manières:

- elles peuvent être obtenues d'un serveur distant (sur un réseau local ou ouvert),
- elles peuvent être stockées en local sur la machine où la vérification est effectuée,
- elles peuvent être stockées avec la signature (en fonction du format).

4.1.1.2 Données de travail

B.Données_A_Vérifier _Hachées

Les données à vérifier formatées sont les données sur lesquelles porte la signature (document et attributs signés), une fois hachées par la TOE.

Protection: intégrité

4.1.1.3 Données en sortie

B.Statut_De_Retour

Après la vérification, la TOE retourne un statut de vérification qui dépend du résultat.

- Signature valide: tous les éléments nécessaires sont présents et corrects.
- Signature invalide: un ou plusieurs sont incorrects.
- Validation incomplète: des données n'étaient pas disponibles au moment de la vérification.

Dans le cas de la vérification immédiate, une validation incomplète doit être comprise par le vérificateur soit comme une signature invalide, soit comme la possibilité de tenter ultérieurement une nouvelle vérification immédiate. Dans le cas de la vérification ultérieure, une validation incomplète doit être comprise par le vérificateur comme une signature invalide.

Protection: intégrité

B.Données_De_Validation_En_Sortie

Les données de validation en sortie sont les données de validation traitées par la TOE.

Elles sont retournées par la TOE au vérificateur pour usage ultérieur.

Ces données peuvent être complètes ou non. Si elles le sont, alors elles pourront servir à une vérification ultérieure. Sinon, elles pourront être réutilisées et enrichies dans le cadre d'une nouvelle vérification immédiate.

Protection: intégrité

4.1.2 Bien sensibles de la TOE (TSF data)

B.Services

Ce bien représente le code exécutable implémentant les services rendus.

Le code de la TOE doit être protégé en intégrité.

Protection: intégrité

B.Règles_De_Vérification

Le coeur de la TOE est constitué d'un moteur vérifiant des règles sur la base d'une politique de signature.

Le code exécutable implantant ces règles dans l'application requiert une protection en intégrité.

Protection: intégrité

B.Politiques_De_Signature

Les politiques de signature définissent les règles à appliquer pour vérifier une signature donnée.

La TOE supporte une ou plusieurs politiques de signature. La liste des politiques de signature, qui est gérée par l'administrateur de la TOE, doit être protégé en intégrité. De plus, l'intégrité de chacune des politiques de signature doit aussi être contrôlée.

Protection: intégrité

Note d'application

En fonction des implémentations, les politiques de signature supportées par la TOE peuvent être sous deux formes:

- sous la forme de code exécutable (séquence d'exécution de règles et d'arbres de décision)
- sous la forme de fichiers interprétables (1) par la TOE, d'une part, et du code exécutable nécessaire à son interprétation, d'autre part. Dans ce cas différents formats peuvent être indifféremment utilisés: normalisés, basés sur ASN.1 ou XML, ou propriétaires.

B.Correspondance_Données_Internes/Externes

Les données internes du module possèdent souvent une représentation différente de celles présentées à l'utilisateur ou entrées dans le module.

La correspondance entre la représentation externe et la représentation interne d'une même donnée nécessite d'être protégée en intégrité.

Ex 1: le type d'engagement (ex: "lu et approuvé") du signataire est représenté en interne par un OID alors qu'il est présenté explicitement au signataire dans l'interface. Ex 2: le format du document entré dans la TOE peut lui aussi être représenté en interne sous la forme d'un OID.

Protection: intégrité

B.Correspondance_FormatDoc_Application

Ce bien est un paramètre géré par la TOE qui lui permet de décider quelle application de présentation externe lancer en fonction du format du document devant être présenté au vérificateur.

L'intégrité de ce bien doit être protégée.

Protection: intégrité

Note d'application

Le format du document est:

- soit fourni par le vérificateur,
- soit présent dans la signature en tant qu'attribut signé.

4.2 Utilisateurs

S.Vérificateur

La TOE peut être invoquée par un être humain ou une application appelante. Le vérificateur désigne l'entité invoquant les fonctions de la TOE pour vérifier une signature.

S.Administrateur_De_Sécurité

L'administrateur de sécurité de la TOE est en charge des opérations suivantes:

- dans le cas où la TOE utilise des politiques de signature paramétrables, il maintient les politiques de signature utilisables (ajout, suppression)
- gère la correspondance entre les formats de document présentés et les applications permettant leur présentation au vérificateur
- gère la liste des formats de document garantissant la stabilité de sémantique du document dans le temps.

Note d'application

Le rôle d'administrateur de sécurité de la TOE est bien distingué du rôle d'administrateur de la machine sur laquelle elle s'exécute (voir l'hypothèse *H.Machine_Hôte*)

4.3 Menaces

Cette section décrit l'ensemble des menaces s'appliquant à la TOE. Puisque tous les objectifs de sécurité découlent des hypothèses et des OSP, la définition des menaces n'est pas nécessaire. Dans ce cas, cette section n'est pas applicable, et elle est donc considérée comme remplie.

4.4 Politiques de sécurité organisationnelles (OSP)

Cette section définit les règles applicables à la TOE.

4.4.1 Politiques relatives à l'application d'une politique de signature

P.Validité_Certificat_Signataire

La TOE doit contrôler que le certificat du signataireétait bien valide au moment où la signature a été positionnée dans le temps.

P.Conformité_Attributs_Signés

La TOE doit contrôler:

- que les attributs signés sont bien conformes à la politique de signature à appliquer, et
- que tous les attributs de signature requis par la politique de signature sont présents.

P.Conformité_Certificat_Signataire

La TOE doit contrôler que tous les certificats du chemin de certification (comprenant le certificat du signataire) sont bien conformes à la politique de signature appliquée.

P.Authenticité_Certificat_Signataire

La TOE doit contrôler qu'un chemin de certification valide (1) existe entre le certificat du signataire et un point de confiance référencé dans la politique de signature.

(1) L'existence d'un tel chemin de validation prouve l'authenticité du certificat du signataire par rapport au certificat racine (point de confiance).

P.Authenticité/Intégrité_Données_Validation

La TOE doit contrôler l'authenticité de l'origine et l'intégrité des données de validation fournies.

4.4.2 Communication des attributs signés

P.Communication_Attributs_Signés

La TOE doit permettre de communiquer les attributs signés au vérificateur.

4.4.3 Présentation du document au vérificateur

P.Possibilité_Présenter_Document

La TOE permettra au vérificateur de visualiser le document signé (Décret 2001-272, Art 5 alinéa c).

Note d'application

Cette capacité sera désactivable par un administrateur de la TOE, pour le cas où le vérificateur est une machine (voir politique P.Administration).

P.Sémantique_Document_Invariante

La TOE doit prévenir le vérificateur si la sémantique du document signé est instable ou peut être instable.

4.4.4 Conformité aux standards

P.Algorithmes_De_Hachage

Le ou les algorithmes de hachage implantés dans la TOE ne doivent pas permettre de créer deux documents produisant le même condensé.

Les algorithmes seront conformes au référentiel cryptographique de la DCSSI [CRYPT-STD].

P.Algorithmes_De_Signature

Les algorithmes cryptographiques supportés et les longueurs des clés mises en oeuvre par la TOE devront résister durant la durée de validité des certificats de clé publique de ces clés.

Les algorithmes seront conformes au référentiel cryptographique de la DCSSI [CRYPT-STD].

Note d'application

Les clés utilisées doivent être conformes au référentiel de gestion de clés de la DCSSI [KEYS-STD].

4.4.5 Export des données de validation

P.Export_Données_Validation

La TOE doit permettre d'exporter au vérificateur les données de validation utilisées lors de la vérification.

4.4.6 Divers

P.Administration

La TOE doit permettre à l'administrateur de sécurité de gérer:

- les politiques de signature [B.Politique_De_Signature] (ajouter/supprimer)
- la table de correspondance entre les applications de visualisation et les formats de documents en entrée de la TOE [B.Correspondance_FormatDoc_Application].
- ainsi que d'inhiber la fonction de visualisation du document signé.

4.5 Hypothèses

Cette section décrit l'ensemble des hypothèses de sécurité sur l'environnement de la TOE.

H.Machine_Hôte

On suppose que la machine hôte sur laquelle la TOE s'exécute est soit directement sous la responsabilité du vérificateur soit sous la responsabilité d'une personne morale ou physique qui lui garantit que les mesures ci-après sont bien appliquées.

Le système d'exploitation de la machine hôte est supposé offrir des contextes d'exécution séparés pour les différentes tâches qu'il exécute.

On suppose de plus que les mesures suivantes sont appliquées:

- la machine hôte est protégée contre les virus
- les échanges entre la machine hôte et d'autres machines via un réseau ouvert sont contrôlés par un pare feu contrôlant et limitant les échanges
- l'accès aux fonctions d'administration de la machine hôte est restreint aux seuls administrateurs de celle-ci (différenciation compte utilisateur/administrateur)
- l'installation et la mise à jour de logiciels sur la machine hôte est sous le contrôle de l'administrateur
- le système d'exploitation de la machine hôte refuse l'exécution d'applications téléchargées ne provenant pas de sources sûres

Note d'application

1) Le rôle d'administrateur de la machine hôte mentionné ci-dessus est distinct de celui d'administrateur de sécurité de la TOE.

2) Cette hypothèse couvre des menaces où des processus informatiques viendraient perturber l'exécution des services de la TOE et par exemple modifier les données utilisateur telles que les certificats et données de validation lorsqu'elles sont sous son contrôle.

H.Politique_Signature_D'Origine_Authentique

L'origine de la ou des politiques de signature utilisables par la TOE est supposée authentique.

Note d'application :

1) Cette hypothèse se justifie ainsi:

Pour vérifier l'authenticité de l'origine d'une politique de signature, il faudrait par exemple vérifier la signature que son émetteur y aurait associé. Pour ce faire, il faudrait alors utiliser une autre politique de signature dont l'authenticité de l'origine resterait à prouver... ce processus serait sans fin.

2) Cette hypothèse est remplie de facto si la TOE n'utilise pas de politiques de signature interprétées mais des politiques fixes.

H.Présentation_Document

On suppose que le système de vérification de signature, dans lequel s'insère la TOE, possède une ou plusieurs applications de présentation qui:

- soit retranscrivent fidèlement le document à vérifier,
- soit préviennent le vérificateur des éventuels problèmes d'incompatibilités du dispositif de présentation avec les caractéristiques du document.

Dans le cas d'une contre-signature, on suppose que l'application de présentation indique au moins l'identité du ou des signataires précédents, et au mieux vérifie cette ou ces signatures.

H.Contrôle_Invariance_Sémantique_Document

On suppose que l'environnement de la TOE fournit un module capable de déterminer si la sémantique du document signé est bien invariante et de communiquer le statut de son analyse à la TOE.

H.Intégrité_Services

On suppose que l'environnement de la TOE fournit à l'administrateur de sécurité les moyens de contrôler l'intégrité des services de la TOE.

H.Accès_Données_De_Validation

La TOE doit disposer de - ou avoir accès à - toutes les données de validation nécessaires à la vérification de la signature d'un document selon la politique de signature à appliquer.

H.Administrateur_De_Sécurité_Sûr

L'administrateur de sécurité de la TOE est supposé être de confiance, formé à l'utilisation de la TOE et disposant des moyens nécessaires à la réalisation de son activité.

Note d'application:

Les hypothèses doivent être réalistes vis-à-vis du produit et de son environnement. Si celles-ci ne sont pas réalistes et ne peuvent notamment pas être déclinées en recommandations dans les manuels, alors la cible de sécurité du produit qui se déclare conforme à ce PP doit les présenter en tant que menaces, et décliner les objectifs de sécurité et exigences de sécurité correspondants.

5 Objectifs de sécurité

5.1 Objectifs de sécurité pour la TOE

5.1.1 Objectifs généraux

O.Administration

La TOE devra permettre à l'administrateur de sécurité de gérer:

- les politiques de signature (ajouter/supprimer)
- la table de correspondance entre les applications de visualisation et les formats de documents en entrée de la TOE.
- ainsi que d'inhiber la fonction de visualisation du document signé.

5.1.2 Objectifs sur les règles de vérification

O.Référence_De_Temps

Conformément à la politique de signature appliquée, la TOE devra s'assurer de la présence d'une référence de temps de confiance qui permette d'attester de l'existence de la signature numérique à une date donnée.

Note d'application

Par référence de temps de confiance on comprend ici tout moyen permettant d'obtenir une référence de temps de manière sure pour le contexte d'utilisation de la TOE. Ce moyen est défini par la politique de signature.

Une référence de temps de confiance peut par exemple être:

- un tampon d'horodatage signé par une entité de confiance, conformément à la politique de signature,
- une marque de temps fournie par un acteur de confiance, conformément à la politique de signature.

O.Chemin_De_Certification

La TOE devra contrôler qu'un chemin de certification valide existe entre:

- le certificat du signataire dont la référence est fournie dans les attributs signés, et
- un point de confiance référencé dans la politique de signature.

O.Conformité_Des_Certificats

La TOE doit vérifier que les certificats du chemin de certification (incluant le certificat du signataire) répondent bien aux critères de la politique de signature appliquée.

O.Validité_Des_Certificats

En conformité avec le RFC 3280, chapitre 6.1, et en conformité avec la politique de signature appliquée, pour chacun des certificats du chemin de certification (incluant le certificat du signataire), la TOE devra vérifier:

- l'intégrité et l'authenticité de l'origine du certificat;

- que le certificat était en cours de validité au moment où la signature numérique a été positionnée dans le temps;
- que le certificat n'était pas révoqué au moment où la signature numérique a été positionnée dans le temps.

O.Conformité_Données_Validation

La TOE doit vérifier que les données de validation fournies pour vérifier la signature répondent bien aux critères de la politique de signature appliquée, notamment qu'elles sont signées par leur émetteur (intégrité et authenticité de l'origine).

Note d'application

La signature des données de validation fournies permet de garantir à la fois l'intégrité de ces données et l'authenticité de leur origine, conformément à la politique de signature appliquée.

O.Conformité_Attributs_Signés

La TOE doit vérifier la présence et la conformité des attributs signés en regard de la politique de signature.

5.1.3 Objectifs relatifs à la visualisation des données signées

O.Lancement_Applications_Présentation

La TOE devra pouvoir lancer des applications externes pour permettre au vérificateur de visualiser le document dont la signature est à vérifier. Pour cela elle se basera sur l'indication du format du document fournie dans la signature électronique à vérifier.

Un paramètre de configuration permettra à un administrateur de la TOE de désactiver cette fonction au moment de l'installation de la TOE si l'utilisateur est une machine.

O.Communication_Attributs_Signés

La TOE devra permettre de communiquer les attributs signés au vérificateur.

Note d'application

Cet objectif s'applique de manière identique aux cas où l'utilisateur est un humain et à celui où c'est une machine et quels que soient les moyens utilisés pour les communiquer: une interface homme/machine ou une interface programmatique (API).

O.Export_Données_Validation

La TOE devra permettre d'exporter au vérificateur les données de validation utilisées lors de la vérification.

5.1.4 Objectifs relatifs au contrôle d'invariance de la sémantique du document à vérifier

O.Invocation_Module_Controle_Invariance

Pour chaque document, la TOE devra interroger un module externe chargé d'identifier si la sémantique du document est bien invariante.

La TOE informera le vérificateur en fonction du résultat transmis par ce module (sémantique invariante, sémantique instable ou sémantique impossible à vérifier).

5.1.5 Conformité aux standards

O.Support_Cryptographique

La TOE devra supporter des algorithmes cryptographiques ayant les propriétés suivantes:

- les algorithmes de hachage ne permettent pas de créer deux documents produisant le même condensé.
- les algorithmes cryptographiques supportés et les longueurs des clés mises en oeuvre par la TOE devront résister durant la durée de validité des certificats de clé publique de ces clés.

Les algorithmes seront conformes au référentiel cryptographique de la DCSSI [CRYPT-STD].

Note d'application

Les clés utilisées doivent être conformes au référentiel de gestion de clés de la DCSSI [KEYS-STD].

5.2 Objectifs de sécurité pour l'environnement opérationnel

OE.Authenticité_Origine_Politique_Signature

Les administrateurs de la TOE devront s'assurer de l'authenticité de l'origine des politiques de signature avant qu'elles ne soient utilisées par la TOE.

OE.Machine_Hôte

La machine hôte sur laquelle la TOE s'exécute devra être soit directement sous la responsabilité du vérificateur soit sous la responsabilité d'une personne morale ou physique qui lui garantit que les mesures ci-après sont bien appliquées.

Le système d'exploitation de la machine hôte devra offrir des contextes d'exécution séparés pour les différentes tâches qu'il exécute.

De plus que les mesures suivantes devront être appliquées:

- la machine hôte est protégée contre les virus;
- les échanges entre la machine hôte et d'autres machines via un réseau ouvert sont contrôlés par un pare feu contrôlant et limitant les échanges;
- l'accès aux fonctions d'administration de la machine hôte est restreint aux seuls administrateurs de celle-ci (différenciation compte utilisateur/administrateur);
- l'installation et la mise à jour de logiciels sur la machine hôte est sous le contrôle de l'administrateur;
- le système d'exploitation de la machine hôte refuse l'exécution d'applications téléchargées ne provenant pas de sources sûres.

Note d'application

Le rôle d'administrateur de la machine hôte mentionné ci-dessus est distinct de celui d'administrateur de sécurité de la TOE.

OE.Présentation_Document

Le système de vérification de signature, dans lequel s'insère la TOE, doit posséder des applications de visualisation qui:

- soit retranscrivent fidèlement le document à vérifier,

- soit préviennent le vérificateur des éventuels problèmes d'incompatibilité du dispositif de présentation avec les caractéristiques du document.

OE.Contrôle_Sémantique_Document_Signé

L'environnement de la TOE devra fournir un module capable de déterminer si la sémantique du document signé:

- soit est bien invariante
- soit est instable
- soit n'a pas pu être vérifiée (par exemple faute de pouvoir supporter ce format).

Ce module doit communiquer le statut de son analyse à la TOE.

OE.Fourniture_Des_Données_De_Validation

L'environnement de la TOE devra lui fournir les données de validation nécessaires à la vérification de la signature.

OE.Intégrité_Services

L'environnement de la TOE devra fournir à l'administrateur de sécurité les moyens de contrôler l'intégrité des services de la TOE.

OE.Administrateur_De_Sécurité_Sûr

L'administrateur de sécurité de la TOE est de confiance, formé à l'utilisation de la TOE et dispose des moyens nécessaires à la réalisation de son activité.

6 Exigences de sécurité

6.1 Exigences de sécurité fonctionnelles

Dans les exigences de sécurité fonctionnelles, les trois termes suivants sont utilisés pour désigner un raffinement:

- *Raffiné éditorialement* (terme défini dans le [CC1]): raffinement dans lequel une modification mineure est faite sur un élément d'exigence, telle que la reformulation d'une phrase pour des raisons de respect de la grammaire anglaise. En aucun cas, cette modification ne doit changer la signification de l'exigence.
- *Raffinement*: raffinement qui permet d'ajouter des précisions ou de limiter l'ensemble des implémentations acceptables pour un élément d'exigence ou à tous les éléments d'exigences d'un même composant.

Le tableau suivant liste les sujets, les objets, les opérations et leurs attributs de sécurité utilisés dans la formulation des exigences de sécurité fonctionnelles:

Subject	Object / Information	Operation	Security attributes
the Verifier	a signed document	import of the document in the TOE	**the Verifier:** - signature policy **the signed document:** - document's stability status
the Verifier	the electronic signature (the signature and the related signed attributes) and the signed document	import of the electronic signature	**the Verifier:** - applied signature policy **the electronic signature:** - signature policy - commitment type - claimed role - presumed signature date and time - presumed signature location **the signed document:** - the signed document's content format
the Verifier	the time reference applied to the signature	import of the time reference	**the Verifier:** - applied signature policy **the time reference applied to the signer's electronic signature:** - the root keys applicable to verify the time-stamp tokens - time-stamp unit certificate - any needed certificate between the certificate and the root key
- the Verifier	- the certificates belonging to a certification path - the revocation data needed to validate the certification path	import of the certificates and the revocation data	**the Verifier:** -applied signature policy **the certificates belonging to a certification path** - key usage - QCStatement - the electronic signaturestatus "correct" - the period of validity of the certificate the time reference - certification policy

Subject	Object / Information	Operation	Security attributes
- the Verifier	- validation status "correct signature"	communication of the status to he verifier	**validation status:** - signer's public key - document's hash - document's electronic signature

6.1.1 Contrôles à l'import du document

FDP_IFC.1 / Document acceptance Subset information flow control

FDP_IFC.1.1 / Document acceptance The TSF shall enforce the **document acceptance information flow control policy** on

- **subjects: the verifier,**
- **information: a signed document**
- **operation: import of the document in the TOE**.

FDP_IFF.1 / Document acceptance Simple security attributes

FDP_IFF.1.1 / Document acceptance The TSF shall enforce the **document acceptance information flow control policy** based on the following types of subject and information security attributes:

- **subjects: the verifier (signature policy, [assignment: verifier's attributes]),**
- **information: the signed document (document's stability status, [assignment: any other document's attributes])**.

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

Import of the document:

- **either the document's stability status equals "stable", or**
- **the document's stability status is "unstable" or "uncontrolled" but the signature policy allows to bypass the control and the verifier explicitly acknowledges to bypass the control**

The Verifier should be informed only if the document's semantics is unstable.

FDP_IFF.1.3 / Document acceptance The TSF shall enforce the **[assignment: additional information flow control SFP rules]**.

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

- **controls succeed**

- o **or controls bypassed**.

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

- o **controls fail**
- o **and controls cannot be bypassed**.

Note d'application

La TOE devra fournir les moyens pour:

- invoquer un vérificateur externe chargé de contrôler l'invariance de la sémantique du document à signer,
- informer le signataire du document si la sémantique n'est pas stable

FDP_ITC.1 / Document acceptance Import of user data without security attributes

FDP_ITC.1.1 / Document acceptance The TSF shall enforce the **document acceptance information flow control policy** when importing user data, controlled under the SFP, from outside of the TOE.

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

FDP_ITC.1.3 / Document acceptance The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **determine whether the document's semantics is invariant or not by invoking a dedicated external module**.

Raffinement:

The TOE shall inform the verifier when the document's semantics is unstable or cannot be checked.

Note d'application

La sémantique d'un document peut par exemple varier lorsque le document contient des champs ou du code actif utilisant des informations exterieures au document.

FMT_MSA.3 / Document's acceptance Static attribute initialisation

FMT_MSA.3.1 / Document's acceptance The TSF shall enforce the **document acceptance access control policy** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

Raffinement:

If the signature policy does not explicitly include a parameter specifying what to do in case the document is not detected as stable, then the default behavior will be to stop the signature process when the document is not detected as stable.

FMT_MSA.3.2/Document's acceptance [Raffiné éditorialement] The TSF shall allow **nobody** to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.1/Document's semantics invariance status Management of security attributes

FMT_MSA.1.1/Document's semantics invariance status [Raffiné éditorialement] The TSF shall enforce the **document acceptance access control policy** to restrict the ability to **modify** the security attribute **document's stability status** to **nobody**.

FMT_SMF.1/Getting document's semantics invariance status Specification of Management Functions

FMT_SMF.1.1/Getting document's semantics invariance status The TSF shall be capable of performing the following management functions:

- **invoking an external module to get the status indicating whether the document's semantics is invariant or not**.

6.1.2 Présentation du document signé

FMT_MTD.1/Document format/viewer association table Management of TSF data

FMT_MTD.1.1/Document format/viewer association table The TSF shall restrict the ability to **modify** the **document format/viewer association table** to **the administrator**.

FMT_SMF.1/Management of the document format/viewer association table Specification of Management Functions

FMT_SMF.1.1/Management of the document format/viewer association table The TSF shall be capable of performing the following management functions:

- **an administrator of the TOE shall be permitted to manage the document format/viewer association table**.

FMT_MTD.1 / Viewer activation parameter Management of TSF data

FMT_MTD.1.1 / Viewer activation parameter The TSF shall restrict the ability to **initialize** the **viewer activation parameter** to **the administrator**.

Raffinement global:

This configuration parameter initialization shall be performed upon the TOE installation.

FMT_SMF.1 / Management of the viewer activation parameter Specification of Management Functions

FMT_SMF.1.1 / Management of the viewer activation parameter The TSF shall be capable of performing the following management functions:

- **the TOE installation procedure shall include the initialization the viewer activation parameter**.

6.1.3 Politiques de signature

6.1.3.1 Sélection de la politique de signature à appliquer

FMT_MTD.1 / Selection of the applied signature policy Management of TSF data

FMT_MTD.1.1 / Selection of the applied signature policy The TSF shall restrict the ability to **select** the **applied signature policy** to **the verifier**.

FMT_SMF.1 / Selection of the applied signature policy Specification of Management Functions

FMT_SMF.1.1 / Selection of the applied signature policy The TSF shall be capable of performing the following management functions:

- **the verifier shall be permitted to select the signature policy to be applied**.

6.1.4 Vérification de la signature

Les exigences qui suivent portent sur le processus de vérification de la signature d'un document.

6.1.4.1 Import de la signature électronique et des attributs signés

Les exigences qui suivent se rapportent à l'import la signature électronique et aux attributs signés.

FDP_IFC.1/Electronic signature Subset information flow control

FDP_IFC.1.1/Electronic signature The TSF shall enforce the **electronic signature information flow control policy** on

- **subjects: the verifier,**
- **information: the electronic signature (the electronic signature and related signed attributes, and the signed document)**
- **operation: import of the electronic signature (i.e. acceptance as signed attributes conforming to the signature policy)**.

Note d'application

Authorizing the import the electronic signature and related signed attributes means that signed attributes meet the rules defined in the applied signature policy.

FDP_IFF.1/Electronic signature Simple security attributes

FDP_IFF.1.1/Electronic signature The TSF shall enforce the **electronic signature information flow control policy** based on the following types of subject and information security attributes:

- **subjects: the verifier (applied signature policy, [assignment: other verifier's attributes, if any])**
- **information: the electronic signature (signature policy, commitment type, claimed role, presumed signature date and time, presumed signature location, [assignment: list of supported signed attributes]) and the signed document (the signed document's content format, [assignment: list of document's attributes])**.

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

Signature import:

- **launch the document viewer corresponding to the document's format, according to the document format/viewer association table, if the viewer activation parameter is set;**
- **inform the verifier if the referenced signature policy is not the applied signature policy, when the electronic signature includes a reference to a signature policy.**
- **if the signed attribute "signature policy" is present in the electronic signature, then its value is conformant to the signature policy;**
- **if the signed attribute "commitment type" is present in the electronic signature, then its value is conformant to the signature policy;**
- **if the signed attribute "claimed role" is present in the electronic signature, then its value is conformant to the signature policy;**
- **if the signed attribute "presumed signature date and time" is present in the electronic signature, then its value is conformant to the signature policy;**

- **if the signed attribute "presumed signature location" is present in the electronic signature then its value is conformant to the signature policy**
- **[assignment: any other supported rule on signed attributes]**.

FDP_IFF.1.3 / Electronic signature The TSF shall enforce the **other rules explicitly defined in the Signature SFP**.

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

- **the signed attributes are compliant with the Signature SFP**
- **and the signed document is stable**.

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

- **the signed attributes are not compliant with the Signature SFP**
- **or the signed document is unstable**.

Note d'application

La TOE devra fournir les moyens pour:

- invoquer un vérificateur externe chargé de contrôler l'invariance de la sémantique du document à signer

FMT_MSA.3 / Electronic signature Static attribute initialisation

FMT_MSA.3.1 / Electronic signature The TSF shall enforce the **electronic signature access control policy** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 / Electronic signature [Raffiné éditorialement] The TSF shall allow **nobody** to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.1 / Electronic signature Management of security attributes

FMT_MSA.1.1 / Electronic signature The TSF shall enforce the **electronic signature access control policy** to restrict the ability to **modify** the security attributes **signature and its signed attributes** to **nobody**.

FDP_ITC.2/Electronic signature Import of user data with security attributes

FDP_ITC.2.1/Electronic signature The TSF shall enforce the **electronic signature information flow control policy** when importing user data, controlled under the SFP, from outside of the TOE.

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

FDP_ITC.2.3/Electronic signature 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/Electronic signature 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/Electronic signature The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE:

- **invoque an external module in charge of controlling the document's semantic invariance (using 1/ the signed document's content format provided by the electronic signature and 2/ the documents' content itself).**
- **transmit the result of the module's analysis to the verifier**.

6.1.4.2 Import d'une réference de temps valide

FDP_IFC.1/Time reference Subset information flow control

FDP_IFC.1.1/Time reference The TSF shall enforce the **time reference acceptance information flow control policy** on

- **subjects: the verifier,**
- **information: the time reference applied to the signature**
- **operation: import of the time reference**.

FDP_IFF.1/Time reference Simple security attributes

FDP_IFF.1.1/Time reference The TSF shall enforce the **time reference acceptance information flow control policy** based on the following types of subject and information security attributes:

- **subjects: the verifier (applied signature policy, [assignment: other verifier's attributes, if any])**
- **information: the time reference applied to the signer's electronic signature (attributes: the root keys applicable to verify the time-stamp**

tokens, time-stamp unit certificate, any needed certificate between the certificate and the root key).

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

Operation: import of the time reference applied to the signer's electronic signature:

- **the key usage of the time-stamping unit certificate indicates that this certificate is only usable for timestamping purposes**
- **there exists a certification path between the time-stamping unit certificate and a root certificate dedicated to the verification of time-stamping tokens**
- **each rule applied to the previously mentioned certification path defined in requirement *FDP_IFF.1/Certification path* is met for the date/time included in the time reference**.

FDP_IFF.1.3/Time reference The TSF shall enforce the **[assignment: additional information flow control SFP rules]**.

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

- **controls succeed**.

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

- **controls fail**.

FMT_MSA.3/Time reference Static attribute initialisation

FMT_MSA.3.1/Time reference The TSF shall enforce the **time reference acceptance access control policy** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/Time reference [Raffiné éditorialement] The TSF shall allow **nobody** to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.1/Time reference Management of security attributes

FMT_MSA.1.1/Time reference The TSF shall enforce the **time reference acceptance access control policy** to restrict the ability to **modify** the security attributes **of the time reference** to **nobody**.

FDP_ITC.2/Time reference Import of user data with security attributes

FDP_ITC.2.1/Time reference The TSF shall enforce the **time reference acceptance information flow control policy** when importing user data, controlled under the SFP, from outside of the TOE.

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

FDP_ITC.2.3/Time reference 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/Time reference 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/Time reference The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **[assignment: additional importation control rules]**.

6.1.4.3 Import d'un chemin de certification valide

Les exigences qui suivent se rapportent aux règles de vérification s'appliquant aux certificats d'un chemin de certification et permettant à l'application de déterminer si le chemin est valide ou non.

Certificats

FMT_MSA.1/Certificates Management of security attributes

FMT_MSA.1.1/Certificates The TSF shall enforce the **certification path acceptance information flow control policy** to restrict the ability to **modify** the security attributes **of the imported certificates** to **nobody**.

Données de validation des certificats

FMT_MSA.1/Certificates' validation data Management of security attributes

FMT_MSA.1.1/Certificates' validation data The TSF shall enforce the **certification path acceptance information flow control policy** to restrict the ability to **modify** the security attributes **of the certificates' revocation data** to **nobody**.

Divers

FDP_IFC.1/Certification path Subset information flow control

FDP_IFC.1.1/Certification path The TSF shall enforce the **certification path acceptance information flow control policy** on

- **subjects: the verifier,**
- **information:**
  - **the certificates belonging to a certification path**
  - **the revocation data needed to validate the certification path**
- **operation: import of the information (i.e. meaning that the path is accepted as a valid certification path according to the signature policy)**.

Note d'application

Authorizing the export of certificates and related validation data means that the path is accepted as a valid certification path according to the signature policy.

FDP_IFF.1/Certification path Simple security attributes

FDP_IFF.1.1/Certification path The TSF shall enforce the **certification path acceptance information flow control policy** based on the following types of subject and information security attributes:

- **subjects: the verifier (applied signature policy, [assignment: other verifier's attributes, if any])**
- **information: certification path validation data, including:**
  - **the certificates belonging to the certification path (certificates' fields): key usage, QCStatement, the electronic signature status, the period of validity, the time reference, certification policy.**
  - **the revocation data of each certificate in the certification path ([assignment: revocation data attributes]),**
  - **[assignment: list of other information checked and, for each, the security attributes]**.

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

Import of the certification path components and related validation data:

- **the certification path binds the signer's certificate to a root certificate defined in the applied signature policy,**

The following rules are met at the date/time included in the imported time reference.

Certification path:

- **for each certificate of the certification path, the electronic signature of the certificate is correct**
- **for each certificate of the certification path, the period of validity of the certificate includes the date included in the time reference**

- **for each revocation data, the electronic signature of the revocation data is correct**
- **for each certificate of the certification path, the certificate is not revocated at the date included in the time reference**
- **for each certificate of the certification path, except the leaf certificate, the key usage indicate that the certificate is a CA certificate**
- **for each certificate of the certification path, the certification policy is conformant with the applied signature policy (application note: there may be different requirements for the CA certificates and for the leaf certificate).**
- **[assignment: any other supported rule on the certification path].**

The following rules are met.

Signer's certificate:

- **the key usage of the signer's certificate indicates that this certificate is usable for non repudiation purposes (Application note: bit 1 of keyUsage set)**
- **the certificate is a Qualified Certificate (Application note: information available using a QCStatement, see RFC 3739),**
- **the private key corresponding to public key is protected by an SCDev (Application note: information available using a QCStatement, see RFC 3739)**
- **[assignment: any other supported rule on signer's certificate fields]**.

FDP_IFF.1.3/Certification path The TSF shall enforce the **[assignment: additional information flow control SFP rules]**.

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

- **controls succeed**.

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

- **controls fail**.

FMT_MSA.3/Certification path Static attribute initialisation

FMT_MSA.3.1/Certification path The TSF shall enforce the **certification path acceptance information flow control policy** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/Certification path [Raffiné éditorialement] The TSF shall allow **nobody** to specify alternative initial values to override the default values when an object or information is created.

FDP_ITC.2/Certification path Import of user data with security attributes

FDP_ITC.2.1/Certification path The TSF shall enforce the **certification path acceptance information flow control policy** when importing user data, controlled under the SFP, from outside of the TOE.

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

FDP_ITC.2.3/Certification path 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/Certification path 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/Certification path The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE:

- **a valid time reference has been imported (see *FDP_IFC.1/Time reference* and associated requirements), in conformance to the applied signature policy;**
- **any data needed to control certificates non repudiation have been imported, in conformance to the applied signature**.

6.1.4.4 Capacité à interpréter les données importées

Les exigences qui suivent porte sur la capacité de la TOE à interpréter les données importées.

FPT_TDC.1/Electronic signature Inter-TSF basic TSF data consistency

FPT_TDC.1.1/Electronic signature The TSF shall provide the capability to consistently interpret **the electronic signature** when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/Electronic signature The TSF shall use **[assignment: list of interpretation rules to be applied by the TSF]** when interpreting the TSF data from another trusted IT product.

Note d'application

Pour instancier l'"assignment" ci-dessus, les rédacteurs de cibles de sécurité devront spécifier les standards supportés par la TOE pour interpréter les signatures électroniques importées (formats de signature supportés).

FPT_TDC.1/Time reference Inter-TSF basic TSF data consistency

FPT_TDC.1.1/Time reference The TSF shall provide the capability to consistently interpret **time references** when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/Time reference The TSF shall use **[assignment: list of interpretation rules to be applied by the TSF]** when interpreting the TSF data from another trusted IT product.

Note d'application

Pour instancier l'"assignment" ci-dessus, les rédacteurs de cibles de sécurité devront spécifier les standards supportés par la TOE permettant d'interpréter les références de temps importées.

FPT_TDC.1/Certificates Inter-TSF basic TSF data consistency

FPT_TDC.1.1/Certificates The TSF shall provide the capability to consistently interpret **certificates** when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/Certificates The TSF shall use **[assignment: list of interpretation rules to be applied by the TSF]** when interpreting the TSF data from another trusted IT product.

Note d'application

Pour instancier l'"assignment" ci-dessus, les rédacteurs de cibles de sécurité devront spécifier les standards supportés par la TOE permettant d'interpréter les certificats importés.

FPT_TDC.1/Certificate revocation data Inter-TSF basic TSF data consistency

FPT_TDC.1.1/Certificate revocation data The TSF shall provide the capability to consistently interpret **certificates' revocation data** when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/Certificate revocation data The TSF shall use **[assignment: list of interpretation rules to be applied by the TSF]** when interpreting the TSF data from another trusted IT product.

Note d'application

Pour instancier l'"assignment" ci-dessus, les rédacteurs de cibles de sécurité devront spécifier les standards supportés par la TOE permettant d'interpréter les données de validation importées.

6.1.4.5 Retour du statut de vérification

FDP_IFC.1 / Electronic signature validation Subset information flow control

FDP_IFC.1.1 / Electronic signature validation The TSF shall enforce the **electronic signature validation information flow policy** on

- **subject: the verifier**
- **information: validation status "correct signature"**
- **operations: communication of the status to the verifier**.

FDP_IFF.1 / Electronic signature validation Simple security attributes

FDP_IFF.1.1 / Electronic signature validation The TSF shall enforce the **electronic signature validation information flow policy** based on the following types of subject and information security attributes:

- **subject: the verifier ([assignment: verifier's security attributes]]**
- **information: validation status "correct signature" (signer's public key, document's hash, document's electronic signature)**.

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

Communication of the status to the verifier:

- **there exists a valid certification path binding the signer's certificate to a root certificate referenced in the applied signature policy and therefore authenticating the signer's public key;**
- **the document's electronic signature, verified using the signer's public key, is correct**
- **to communicate the status "wrong signature" in case at least one rule among the information control policy rules is false**.

FDP_IFF.1.3 / Electronic signature validation The TSF shall enforce the **[assignment: additional information flow control SFP rules]**.

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

- **controls succeed**.

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

- **controls fail**.

FMT_MSA.3 / Signature validation status Static attribute initialisation

FMT_MSA.3.1 / Signature validation status The TSF shall enforce the **electronic signature validation information flow policy** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 / Signature validation status The TSF shall allow the **nobody** to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.1 / Signature validation status Management of security attributes

FMT_MSA.1.1 / Signature validation status The TSF shall enforce the **electronic signature validation information flow policy** to restrict the ability to **modify** the security attributes **signature validation status** to **nobody**.

FDP_ETC.2 / Verification status Export of user data with security attributes

FDP_ETC.2.1 / Verification status The TSF shall enforce the **electronic signature validation information flow policy** when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.2.2 / Verification status The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3 / Verification status The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.

FDP_ETC.2.4 / Verification status The TSF shall enforce the following rules when user data is exported from the TOE:

- **data exported as security attributes of the verification status are:**
  - **the validation data contributing to prove the verification status correctness,**
  - **the signed attributes,**
  - **the limit on the value of transactions for which the signer's certificate can be used, if it is specified in the signer's certificate, and**
  - **the result of the analysis of the document's semantics invariance to the verifier**.

Note d'application

Les données de validation sont destinées à être éventuellement réutilisées lors d'une vérification ultérieure.

Les attributs signés, la limitation sur le montant de la transaction et la stabilité de la sémantique du document sont communiqués au vérificateur par une interface programmatique ou une interface homme/machine.

6.1.5 Support cryptographique

FCS_COP.1 / Signature verification Cryptographic operation

FCS_COP.1.1 / Signature verification The TSF shall perform

- **electronic signature verification** in accordance with a specified cryptographic algorithm **[assignment: cryptographic algorithm]** and cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **CRYPT-STD, [assignment: list of standards]**.

Raffinement global:

The ST author must choose cryptographic algorithms having key lengths resistant to a cryptanalysis attacks. The public-private key pairs used by those algorithms shall be strong enough to thwart attacks during the validity period of the certificate to which the public key is linked.

Note d'application

Les clés utilisées doivent être conformes au référentiel de gestion de clés de la DCSSI [KEYS-STD].

FCS_COP.1 / Hash Cryptographic operation

FCS_COP.1.1 / Hash The TSF shall perform

- **hash generation** in accordance with a specified cryptographic algorithm **[assignment: hash algorithm]** and cryptographic key sizes **[assignment: hash size]** that meet the following: **CRYPT-STD, [assignment: list of standards]**.

Raffinement global:

The ST author must select a hash generating algorithm which does not produce identical message-digests out of two distinct documents.

6.1.6 Identification et authentification de l'utilisateur

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles

- **verifier**
- **administrator**.

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.

Note d'application

Le mechanisme d'authentification doit être conforme au référentiel d'authentification de la DCSSI [AUTH-STD].

6.2 Exigences de sécurité d'assurance

Le niveau des exigences d'assurance de sécurité est EAL3 augmenté de ALC_FLR.3 et AVA_VAN.3.

7 Argumentaires

7.1 Objectifs de sécurité / problème de sécurité

7.1.1 Politiques de sécurité organisationnelles (OSP)

7.1.1.1 Politiques relatives à l'application d'une politique de signature

P.Validité_Certificat_Signataire La politique de sécurité organisationnelle *P.Validité_Certificat_Signataire* est couverte par les objectifs de sécurité sur la TOE:

- *O.Référence_De_Temps* qui requiert que la signature soit positionnée dans le temps
- *O.Validité_Des_Certificats* qui requiert que la TOE vérifie que le certificat du signataire utilisé pour la signature était bien valide au moment où la signature a été positionnée dans le temps.

P.Conformité_Attributs_Signés La politique de sécurité organisationnelle *P.Conformité_Attributs_Signés* est complètement couverte par l'objectif de sécurité sur la TOE *O.Conformité_Attributs_Signés* qui en reprend les éléments.

P.Conformité_Certificat_Signataire La politique de sécurité organisationnelle *P.Conformité_Des_Certificats* est couverte par l'objectif de sécurité sur la TOE *O.Conformité_Des_Certificats* qui en reprend les éléments.

P.Authenticité_Certificat_Signataire La politique de sécurité organisationnelle *P.Authenticité_Certificat_Signataire* est couverte par l'objectif de sécurité sur la TOE *O.Chemin_De_Certification* qui requiert que la TOE contrôle qu'un chemin de certification valide existe pour attester l'authenticité du certificat du signataire utilisé pour la signature.

P.Authenticité/Intégrité_Données_Validation La politique de sécurité organisationnelle *P.Authenticité/Intégrité_Données_De_Validation* est couverte par l'objectif de sécurité *O.Conformité_Données_Validation* qui requiert notamment que ces données soient signées par leur émetteur.

7.1.1.2 Communication des attributs signés

P.Communication_Attributs_Signés La politique de sécurité organisationnelle *P.Communication_Attributs_Signés* est couverte par l'objectif *O.Communication_Attributs_Signés* qui exige que la TOE présente les attributs signés au vérificateur.

7.1.1.3 Présentation du document au vérificateur

P.Possibilité_Présenter_Document La politique de sécurité organisationnelle *P.Possibilité_Présenter_Document* est couverte par les objectifs de sécurité suivants:

- *OE.Présentation_Document* qui requiert que l'environnement de la TOE fournisse une application permettant au vérificateur de visualiser le document signé.
- *O.Lancement_Applications_Présentation* qui requiert d'une part que la TOE puisse lancer une application de visualisation fournie par l'environnement de la TOE sur demande du vérificateur, d'autre part que cette fonctionnalité puisse être inhibée au moment de l'installation.

P.Sémantique_Document_Invariante La politique de sécurité organisationnelle *P.Sémantique_Du_Document_Invariante* est couverte d'une part par l'objectif de sécurité sur la TOE *O.Invocation_Module_Controle_Invariance* qui requiert que la TOE interroge un module externe chargé de contrôler l'invariance de la sémantique du document signé et communique le résultat du contrôle au vérificateur, d'autre part par l'objectif de sécurité sur l'environnement *OE.Contrôle_Sémantique_Document_Signé* qui requiert que l'environnement de la TOE fournisse un tel module.

7.1.1.4 Conformité aux standards

P.Algorithmes_De_Hachage La politique de sécurité organisationnelle *P.Algorithme_De_Hachage* est directement couverte par l'objectif de sécurité *O.Support_Cryptographique* qui, sur ce point, en reprend les éléments.

P.Algorithmes_De_Signature La politique de sécurité organisationnelle *P.Algorithmes_De_Signature* est directement couverte par l'objectif de sécurité *O.Support_Cryptographique* qui, sur ce point, en reprend tous les éléments.

7.1.1.5 Export des données de validation

P.Export_Données_Validation Cette politique est couverte par l'objectif *O.Export_Données_Validation* qui reprend tous les éléments de celle-ci.

7.1.1.6 Divers

P.Administration Cette politique est couverte par l'objectif *O.Administration* qui en reprend les termes et d'autre part par l'objectif de sécurité sur l'environnement *OE.Administrateur_De_Sécurité_Sûr* qui assure que l'administrateur de la TOE n'est pas un agent menaçant.

7.1.2 Hypothèses

H.Machine_Hôte L'hypothèse *H.Machine_Hôte* est couverte par l'objectif de sécurité sur l'environnement *OE.Machine_Hôte* qui en reprend les éléments.

H.Politique_Signature_D'Origine_Authentique L'hypothèse *H.Politique_De_Signature_D'Origine_Authentique* est couverte par l'objectif de sécurité sur l'environnement *OE.Authenticité_Origine_Politique_Signature* demandant aux administrateurs de la TOE de s'assurer de l'authenticité de l'origine des politiques de signature utilisables par la TOE.

H.Présentation_Document L'hypothèse *H.Présentation_Document* est couverte par l'objectif de sécurité sur l'environnement *OE.Présentation_Document* qui en reprend les éléments.

H.Contrôle_Invariance_Sémantique_Document L'hypothèse *H.Contrôle_Invariance_Sémantique_Document* est couverte par l'objectif de sécurité sur l'environnement *OE.Contrôle_Sémantique_Document_Signé* qui en reprend les éléments.

H.Intégrité_Services L'hypothèse *H.Intégrité_Services* est couverte entièrement par l'objectif sur l'environnement *OE.Intégrité_Services* qui en reprend les termes.

H.Accès_Données_De_Validation La politique de sécurité organisationnelle *H.Accès_Données_De_Validation* est couverte par l'objectif sur l'environnement *OE.Fourniture_Des_Données_De_Validation* qui requiert que ce dernier fournisse les données de validation nécessaires à la vérification de la signature.

H.Politique_SIgnature_D'Origine_Authentique L'hypothèse *H.Politique_De_Signature_D'Origine_Authentique* est couverte par l'objectif de sécurité sur l'environnement *OE.Authenticité_Origine_Politique_Signature* demandant aux administrateurs de la TOE de s'assurer de l'authenticité de l'origine des politiques de signature utilisables par la TOE.

H.Administrateur_De_Sécurité_Sûr L'hypothèse *H.Administrateur_De_Sécurité_Sûr* est couverte entièrement par l'objectif sur l'environnement *OE.Administrateur_De_Sécurité_Sûr* qui en reprend les termes.

7.1.3 Tables de couverture entre définition du problème et objectifs de sécurité

Politiques de sécurité organisationnelles (OSP)	Objectifs de sécurité	Argumentaire
P.Validité_Certificat_Signataire	O.Référence_De_Temps, O.Validité_Des_Certificats	Section 7.1.1
P.Conformité_Attributs_Signés	O.Conformité_Attributs_Signés	Section 7.1.1
P.Conformité_Certificat_Signataire	O.Conformité_Des_Certificats	Section 7.1.1
P.Authenticité_Certificat_Signataire	O.Chemin_De_Certification	Section 7.1.1
P.Authenticité/Intégrité_Données_Validation	O.Conformité_Données_Validation	Section 7.1.1
P.Communication_Attributs_Signés	O.Communication_Attributs_Signés	Section 7.1.1
P.Possibilité_Présenter_Document	OE.Présentation_Document, O.Lancement_Applications_Présentation	Section 7.1.1
P.Sémantique_Document_Invariante	O.Invocation_Module_Controle_Invariance, OE.Contrôle_Sémantique_Document Signé	Section 7.1.1

Politiques de sécurité organisationnelles (OSP)	Objectifs de sécurité	Argumentaire
P.Algorithmes_De_Hachage	O.Support_Cryptographique	Section 7.1.1
P.Algorithmes_De_Signature	O.Support_Cryptographique	Section 7.1.1
P.Export_Données_Validation	O.Export_Données_Validation	Section 7.1.1
P.Administration	O.Administration, OE.Administrateur_De_Sécurité_Sûr	Section 7.1.1

Tableau 2 Association politiques de sécurité organisationnelles vers objectifs de sécurité

Objectifs de sécurité	Politiques de sécurité organisationnelles (OSP)
O.Administration	P.Administration
O.Référence_De_Temps	P.Validité_Certificat_Signataire
O.Chemin_De_Certification	P.Authenticité_Certificat_Signataire
O.Conformité_Des_Certificats	P.Conformité_Certificat_Signataire
O.Validité_Des_Certificats	P.Validité_Certificat_Signataire
O.Conformité_Données_Validation	P.Authenticité/Intégrité_Données_Validation
O.Conformité_Attributs_Signés	P.Conformité_Attributs_Signés
O.Lancement_Applications_Présentation	P.Possibilité_Présenter_Document
O.Communication_Attributs_Signés	P.Communication_Attributs_Signés
O.Export_Données_Validation	P.Export_Données_Validation
O.Invocation_Module_Controle_Invariance	P.Sémantique_Document_Invariante
O.Support_Cryptographique	P.Algorithmes_De_Hachage, P.Algorithmes_De_Signature
OE.Authenticité_Origine_Politique_Signature	
OE.Machine_Hôte	
OE.Présentation_Document	P.Possibilité_Présenter_Document
OE.Contrôle_Sémantique_Document_Signé	P.Sémantique_Document_Invariante
OE.Fourniture_Des_Données_De_Validation	
OE.Intégrité_Services	
OE.Administrateur_De_Sécurité_Sûr	P.Administration

Tableau 3 Association objectifs de sécurité vers politiques de sécurité organisationnelles

Hypothèses	Objectifs de sécurité pour l'environnement opérationnel	Argumentaire
H.Machine_Hôte	OE.Machine_Hôte	Section 7.1.2
H.Politique_Signature_D'Origine_Authentique	OE.Authenticité_Origine_Politique_Signature	Section 7.1.2
H.Présentation_Document	OE.Présentation_Document	Section 7.1.2
H.Contrôle_Invariance_Sémantique_Document	OE.Contrôle_Sémantique_Document Signé	Section 7.1.2
H.Intégrité_Services	OE.Intégrité_Services	Section 7.1.2
H.Accès_Données_De_Validation	OE.Fourniture_Des_Données_De_Validation	Section 7.1.2
H.Administrateur_De_Sécurité_Sûr	OE.Administrateur_De_Sécurité_Sûr	Section 7.1.2

Tableau 4 Association hypothèses vers objectifs de sécurité pour l'environnement opérationnel

Objectifs de sécurité pour l'environnement opérationnel	Hypothèses
OE.Authenticité_Origine_Politique_Signature	H.Politique_Signature_D'Origine_Authentique
OE.Machine_Hôte	H.Machine_Hôte
OE.Présentation_Document	H.Présentation_Document
OE.Contrôle_Sémantique_Document_Signé	H.Contrôle_Invariance_Sémantique_Document
OE.Fourniture_Des_Données_De_Validation	H.Accès_Données_De_Validation
OE.Intégrité_Services	H.Intégrité_Services
OE.Administrateur_De_Sécurité_Sûr	H.Administrateur_De_Sécurité_Sûr

Tableau 5 Association objectifs de sécurité pour l'environnement opérationnel vers hypothèses

7.2 Exigences de sécurité / objectifs de sécurité

7.2.1 Objectifs

7.2.1.1 Objectifs de sécurité pour la TOE

Objectifs généraux

O.Administration Cet objectif est couvert par les exigences fonctionnelles suivantes:

- *FMT_SMF.1/Management of the document format/viewer association table* qui définit la fonction d'administration des données d'association entre les formats de documents signés et les applications de visualisation.
- *FMT_SMF.1/Management of the viewer activation parameter* qui définit la fonction permettant d'inhiber la fonction de visualisation du document signé

Objectifs sur les règles de vérification

O.Référence_De_Temps L'objectif de sécurité *O.Référence_De_Temps* est couvert de la manière suivante:

La TOE doit appliquer une politique de contrôle de flux d'informations (*FDP_IFC.1/Time reference*) lors de l'import de la référence de temps associée à la signature numérique pour accepter cette référence comme valide. Le composant fonctionnel *FDP_IFF.1/Time reference* définit les règles à appliquer sur les différentes données mises en jeu pour déterminer si la référence de temps est valide; certaines règles portent sur la référence de temps elle-même, d'autres portent sur les données de validation de cette référence. Ce composant liste en plus l'ensemble de règles applicables aux données de validation sont définies au sein du composant fonctionnel; selon la politique de signature appliquée, un sous-ensemble de ces règles sera effectivement appliqué.

Les composants fonctionnels *FMT_MTD.1/Selection of the applied signature policy* et *FMT_SMF.1/Selection of the applied signature policy* définissent que seul le vérificateur peut sélectionner la politique de signature à appliquer.

Les composants fonctionnels *FDP_ITC.2/Time reference* et *FPT_TDC.1/Time reference* assurent d'une part que la TOE applique la politique de contrôle de flux lors de l'import de la référence de temps et d'autre part que la TOE est en mesure d'interpréter les données importées et donc de les exploiter.

Les composants fonctionnels suivants, portant sur la gestion des attributs de sécurité des sujets et informations mis en jeu dans la politique de contrôle de flux contribuent eux aussi à couvrir cet objectif:

- Le composant fonctionnel *FMT_MSA.3/Time reference* garantit que les valeurs par défaut attribuées aux attributs de sécurité mis en jeu dans la politique de contrôle de flux prennent des valeurs restrictives.
- Le composant fonctionnel *FMT_MSA.1/Time reference* garantit la non modification des attributs de sécurité de la référence de temps.
- Le composant fonctionnel *FMT_MSA.1/Certificates* garantit la non modification des attributs des certificats impliqués dans la vérification de la validité de la référence de temps.
- Le composant fonctionnel *FMT_MSA.1/Certificates' validation data* garantit la non modification des attributs des données de validation des certificats impliqués dans le contrôle de la validité de la référence de temps.

- Le composant *FMT_SMR.1* demande à la TOE de différencier le rôle de vérificateur du rôle d'administrateur.
- Le composant *FIA_UID.2* requiert que la TOE ne permette la réalisation d'aucune opération avant d'avoir identifié avec succès l'utilisateur.

O.Chemin_De_Certification L'objectif de sécurité *O.Chemin_De_Certification* est couvert de la manière suivante:

La TOE doit appliquer une politique de contrôle de flux d'informations (*FDP_IFC.1/Certification path*) lors de l'import d'un ensemble de certificats constituant un chemin de certification entre le certificat du signataire et un certificat racine défini dans la politique de signature.

Le composant fonctionnel *FDP_ITC.2/Certification path* assure que la TOE applique la politique de contrôle de flux lors de l'import des certificats. Les composants *FPT_TDC.1/Certificates* et *FPT_TDC.1/Certificate revocation data* assurent que la TOE est bien en mesure d'exploiter ces données.

Les règles de la politique de contrôle de flux sont définies dans le composant fonctionnel *FDP_IFF.1/Certification path*. Ce composant définit l'ensemble des règles devant être implémentées.

Les règles à vérifier pour assurer la validité du chemin de certification sont définies par la politique de signature appliquée. Cette politique ne peut être choisie que par le vérificateur (*FMT_MTD.1/Selection of the applied signature policy* et *FMT_SMF.1/Selection of the applied signature policy*).

Les composants fonctionnels suivants, portant sur la gestion des attributs de sécurité des sujets et informations mis en jeu dans la politique de contrôle de flux contribuent eux aussi à couvrir cet objectif:

- Le composant fonctionnel *FMT_MSA.3/Certification path* garantit que les valeurs par défaut attribuées aux attributs de sécurité mis en jeu dans la politique de contrôle de flux prennent des valeurs restrictives.
- Le composant fonctionnel *FMT_MSA.1/Certificates* garantit la non modification des attributs des certificats importés pour construire le chemin de certification.
- Le composant fonctionnel *FMT_MSA.1/Certificates' validation data* garantit la non modification des attributs des données de validation du certificat du signataire.

Enfin les composants suivants contribuent à la bonne application de la politique de contrôle de flux:

- Le composant *FMT_SMR.1* demande à la TOE de différencier le rôle de vérificateur du rôle d'administrateur.
- Le composant *FIA_UID.2* requiert que la TOE ne permette la réalisation d'aucune opération avant d'avoir identifié avec succès l'utilisateur.

O.Conformité_Des_Certificats L'objectif de sécurité *O.Conformité_Des_Certificats* est couvert de la manière suivante:

La TOE doit appliquer une politique de contrôle de flux d'informations (*FDP_IFC.1/Certification path*) lors de l'import d'un ensemble de certificats constituant un chemin de certification entre le certificat du signataire et un certificat racine défini dans la politique de signature.

Le composant fonctionnel *FDP_ITC.2/Certification path* assure que la TOE applique la politique de contrôle de flux lors de l'import des certificats. Les composants

FPT_TDC.1/Certificates et *FPT_TDC.1/Certificate revocation data* assurent que la TOE est bien en mesure d'exploiter ces données.

Les règles de la politique de contrôle de flux sont définies dans le composant fonctionnel *FDP_IFF.1/Certification path* qui indique l'ensemble des règles devant être implémentées.

Les règles à vérifier pour assurer la validité du chemin de certification sont définies par la politique de signature appliquée. Cette politique ne peut être choisie que par le vérificateur (*FMT_MTD.1/Selection of the applied signature policy* et *FMT_SMF.1/Selection of the applied signature policy*).

Les composants fonctionnels suivants, portant sur la gestion des attributs de sécurité des sujets et informations mis en jeu dans la politique de contrôle de flux contribuent eux aussi à couvrir cet objectif:

- Le composant fonctionnel *FMT_MSA.3/Certification path* garantit que les valeurs par défaut attribuées aux attributs de sécurité mis en jeu dans la politique de contrôle de flux prennent des valeurs restrictives.
- Le composant fonctionnel *FMT_MSA.1/Certificates* garantit la non modification des attributs des certificats importés pour construire le chemin de certification.
- Le composant fonctionnel *FMT_MSA.1/Certificates' validation data* garantit la non modification des attributs des données de validation du certificat du signataire.

Enfin les composants suivants contribuent à la bonne application de la politique de contrôle de flux:

- Le composant *FMT_SMR.1* demande à la TOE de différencier le rôle de vérificateur du rôle d'administrateur.
- Le composant *FIA_UID.2* requiert que la TOE ne permette la réalisation d'aucune opération avant d'avoir identifié avec succès l'utilisateur.

O.Validité_Des_Certificats L'objectif de sécurité *O.Validité_Des_Certificats* est couvert de la manière suivante:

La TOE doit appliquer une politique de contrôle de flux d'informations (*FDP_IFC.1/Certification path*) lors de l'import d'un ensemble de certificats constituant un chemin de certification entre le certificat du signataire et un certificat racine défini dans la politique de signature.

Le composant fonctionnel *FDP_ITC.2/Certification path* assure que la TOE applique la politique de contrôle de flux lors de l'import des certificats et des informations de non révocation.

Les composants *FPT_TDC.1/Certificates* et en particulier *FPT_TDC.1/Certificate revocation data* assurent que la TOE est bien en mesure d'exploiter ces données.

Les règles de la politique de contrôle de flux sont définies dans le composant fonctionnel *FDP_IFF.1/Certification path*. Ce composant indique l'ensemble des règles devant être implémentées. Cette exigence comportent notamment des règles permettant à la TSF de s'assurer que les certificats du chemin sont bien en cours de validité et que leur état est non révoqué.

Les règles à vérifier effectivement pour assurer la validité des certificats du chemin sont définies par la politique de signature appliquée. Cette politique ne peut être choisie que par le vérificateur (*FMT_MTD.1/Selection of the applied signature policy* et *FMT_SMF.1/Selection of the applied signature policy*).

Les composants fonctionnels suivants, portant sur la gestion des attributs de sécurité des sujets et informations mis en jeu dans la politique de contrôle de flux contribuent eux aussi à couvrir cet objectif:

- Le composant fonctionnel *FMT_MSA.3/Certification path* garantit que les valeurs par défaut attribuées aux attributs de sécurité mis en jeu dans la politique de contrôle de flux prennent des valeurs restrictives.
- Le composant fonctionnel *FMT_MSA.1/Certificates* garantit la non modification des attributs des certificats importés pour construire le chemin de certification.
- Le composant fonctionnel *FMT_MSA.1/Certificates' validation data* garantit la non modification des attributs des données de validation du certificat du signataire.

Enfin les composants suivants contribuent à la bonne application de la politique de contrôle de flux:

- Le composant *FMT_SMR.1* demande à la TOE de différencier le rôle de vérificateur du rôle d'administrateur.
- Le composant *FIA_UID.2* requiert que la TOE ne permette la réalisation d'aucune opération avant d'avoir identifié avec succès l'utilisateur.

O.Conformité_Données_Validation L'objectif de sécurité *O.Conformité_Données_Validation* est couvert de la manière suivante:

La TOE doit appliquer une politique de contrôle de flux d'informations (*FDP_IFC.1/Certification path*) lors de l'import d'un ensemble de certificats constituant un chemin de certification entre le certificat du signataire et un certificat racine défini dans la politique de signature. Cette politique de contrôle de flux s'applique aussi aux informations de non-révocation associées aux certificats.

Le composant fonctionnel *FDP_ITC.2/Certification path* assure que la TOE applique la politique de contrôle de flux lors de l'import des certificats et des informations de non révocation.

Les composants *FPT_TDC.1/Certificates* et en particulier *FPT_TDC.1/Certificate revocation data* assurent que la TOE est bien en mesure d'exploiter ces données.

Les règles de la politique de contrôle de flux sont définies dans le composant fonctionnel *FDP_IFF.1/Certification path*. Ce dernier composant indique l'ensemble des règles devant être implémentées et comporte des règles permettant à la TSF de s'assurer de la validité les données de révocation des certificats.

Les règles à vérifier pour assurer la validité des informations de révocation des certificats du chemin sont définies par la politique de signature appliquée. Cette politique ne peut être choisie que par le vérificateur (*FMT_MTD.1/Selection of the applied signature policy* et *FMT_SMF.1/Selection of the applied signature policy*).

Les composants fonctionnels suivants, portant sur la gestion des attributs de sécurité des sujets et informations mis en jeu dans la politique de contrôle de flux contribuent eux aussi à couvrir cet objectif:

- Le composant fonctionnel *FMT_MSA.3/Certification path* garantit que les valeurs par défaut attribuées aux attributs de sécurité mis en jeu dans la politique de contrôle de flux prennent des valeurs restrictives.
- Le composant fonctionnel *FMT_MSA.1/Certificates* garantit la non modification des attributs des certificats importés pour construire le chemin de certification.
- Le composant fonctionnel *FMT_MSA.1/Certificates' validation data* garantit la non modification des attributs des données de validation du certificat du signataire.

Enfin les composants suivants contribuent à la bonne application de la politique de contrôle de flux:

- Le composant *FMT_SMR.1* demande à la TOE de différencier le rôle de vérificateur du rôle d'administrateur.

- Le composant *FIA_UID.2* requiert que la TOE ne permette la réalisation d'aucune opération avant d'avoir identifié avec succès l'utilisateur.

O.Conformité_Attributs_Signés L'objectif de sécurité *O.Conformité_Des_Attributs_Signés* est couvert de la manière suivante:

La TOE doit appliquer une politique de contrôle de flux d'informations au moment de l'import de la signature électronique (*FDP_IFC.1/Electronic signature*). Le composant fonctionnel *FDP_IFF.1/Electronic signature* définit les règles à appliquer notamment pour contrôler la conformité des attributs signés vis-à-vis de la politique de signature. Ce dernier composant définit également l'ensemble des règles devant être implémentées par la TOE. La politique de signature appliquée invoque un sous ensemble de ces règles.

Les composants fonctionnels *FMT_MTD.1/Selection of the applied signature policy* et *FMT_SMF.1/Selection of the applied signature policy* définissent que seul le vérificateur peut sélectionner la politique de signature à appliquer.

Les composants fonctionnels *FDP_ITC.2/Electronic signature* et *FPT_TDC.1/Electronic signature* assurent d'une part que la TOE applique la politique de contrôle de flux lors de l'import de la signature électronique (comportant des attributs signés) et d'autre part que la TOE est bien en mesure d'interpréter et donc d'exploiter ces données.

Les composants fonctionnels suivants, portant sur la gestion des attributs de sécurité des sujets et informations mis en jeu dans la politique de contrôle de flux contribuent eux aussi à couvrir cet objectif:

- Le composant fonctionnel *FMT_MSA.3/Electronic signature* garantit que les valeurs par défaut attribuées aux attributs de sécurité mis en jeu dans la politique de contrôle de flux prennent des valeurs restrictives.
- Le composant fonctionnel *FMT_MSA.1/Electronic signature* garantit la non modification des attributs de la signature.

Enfin les composants suivants contribuent à la bonne application de la politique de contrôle de flux:

- Le composant *FMT_SMR.1* demande à la TOE de différencier le rôle de vérificateur du rôle d'administrateur.
- Le composant *FIA_UID.2* requiert que la TOE ne permette la réalisation d'aucune opération avant d'avoir identifié avec succès l'utilisateur.

Objectifs relatifs à la visualisation des données signées

O.Lancement_Applications_Présentation L'objectif de sécurité *O.Lancement_Applications_Présentation* est couvert par les composants d'exigence suivants:

- *FDP_IFF.1/Electronic signature*, qui assure que l'utilisateur pourra visualiser le document à travers une application de visualisation externe. La TOE lance automatiquement l'application de visualisation associée au format du document à signer en utilisant une *liste d'associations format document/visualisateur*.
- *FMT_MTD.1/Document format/viewer association table* et *FMT_SMF.1/Management of the document format/viewer association table* qui garantissent que le contenu de la *liste d'associations format document/visualisateur* ne peut être modifiée que par un administrateur.
- *FMT_MTD.1/Viewer activation parameter* et *FMT_SMF.1/Management of the viewer activation parameter* qui garantissent que le *paramètre d'activation de la*

fonction de visualisation du document signé ne peut être modifiée que par un administrateur.

O.Communication_Attributs_Signés L'objectif de sécurité *O.Communication_Attributs_Signés* est couvert par les composants d'exigence suivants:

- *FDP_IFF.1/Electronic signature*, qui requiert que la TOE soit capable d'exporter les attributs de la signature.

O.Export_Données_Validation L'objectif de sécurité *O.Communication_Données_De_Validation* est couvert de la manière suivante:

La TOE doit appliquer une politique de contrôle de flux d'informations au moment d'exporter le résultat de la vérification de la signature (*FDP_IFC.1/Electronic signature validation* et *FDP_IFF.1/Electronic signature validation*).

Le composant fonctionnel *FDP_ETC.2/Verification status* requiert que le statut de vérification de la signature soit communiqué avec les données de validation prouvant son exactitude et avec les informations nécessaires au vérificateur pour traiter la signature (attributs signés, champs du certificat du signataire,...)

Les composants fonctionnels suivants, portant sur la gestion des attributs de sécurité des sujets et informations mis en jeu dans la politique de contrôle de flux contribuent eux aussi à couvrir cet objectif:

- Le composant fonctionnel *FMT_MSA.3/Signature validation status* garantit que les valeurs par défaut attribuées aux attributs de sécurité mis en jeu dans la politique de contrôle de flux prennent des valeurs restrictives.
- Le composant fonctionnel *FMT_MSA.1/Signature validation status* garantit la non modification du statut de la signature.

Enfin les composants suivants contribuent à la bonne application de la politique de contrôle de flux:

- Le composant *FMT_SMR.1* demande à la TOE de différencier le rôle de vérificateur du rôle d'administrateur.
- Le composant *FIA_UID.2* requiert que la TOE ne permette la réalisation d'aucune opération avant d'avoir identifié avec succès l'utilisateur.

Objectifs relatifs au contrôle d'invariance de la sémantique du document à vérifier

O.Invocation_Module_Controle_Invariance L'objectif de sécurité *O.Invocation_Module_Contrôle_Invariance* est couvert de la manière suivante:

La TOE doit appliquer une politique de contrôle de flux d'informations lors de l'import d'un document dans le champ de contrôle de la TOE (*FDP_IFC.1/Document acceptance*). Le composant fonctionnel *FDP_IFF.1/Document acceptance* définit les règles à appliquer par la TOE pour accepter le document.

Le composant *FDP_ITC.1/Document acceptance* requiert que la TOE invoque un module externe pour déterminer si la sémantique du document est stable ou non, au moment où elle importe le document.

Les composants fonctionnels suivants, portant sur la gestion des attributs de sécurité des sujets et informations mis en jeu dans la politique de contrôle de flux contribuent eux aussi à couvrir cet objectif:

- Le composant fonctionnel *FMT_MSA.3/Document's acceptance* garantit que les valeurs par défaut attribuées aux attributs de sécurité mis en jeu dans la politique de contrôle de flux prennent des valeurs restrictives.
- Les composants fonctionnels *FMT_MSA.1/Document's semantics invariance status* et *FMT_SMF.1/Getting document's semantics invariance status* qui requièrent d'une part que la TOE dispose d'un moyen d'invoquer un module externe pour obtenir le statut définissant si la sémantique du document est stable, d'autre part que personne ne puisse modifier ce statut une fois obtenu.
- Le composant *FMT_SMR.1* demande à la TOE de différencier le rôle de signataire du rôle d'administrateur.
- Le composant *FIA_UID.2* requiert que la TOE ne permette la réalisation d'aucune opération avant d'avoir identifié avec succès l'utilisateur.

Conformité aux standards

O.Support_Cryptographique L'objectif de sécurité *O.Support_Cryptographique* est couvert par les exigences:

- *FCS_COP.1/Hash* pour ce qui concerne la propriété de non collision entre les condensés formatés produits par l'application de l'algorithme de hachage.
- *FCS_COP.1/Signature verification* qui garantit que tous les algorithmes cryptographiques utilisés dans le processus de vérification de la signature électronique sont résistants aux attaques par cryptanalyse. En particulier la taille des clefs devra être suffisamment grande pour assurer la résistance de la clef publique présente dans un certificat pendant la durée de validité de ce dernier.

7.2.2 Tables de couverture entre objectifs et exigences de sécurité

Objectifs de sécurité	Exigences fonctionnelles pour la TOE	Argumentaire
O.Administration	FMT_SMF.1/Management of the viewer activation parameter, FMT_SMF.1/Management of the document format/viewer association table	Section 7.2.1
O.Référence_De_Temps	FDP_IFC.1/Time reference, FDP_IFF.1/Time reference, FMT_MTD.1/Selection of the applied signature policy, FMT_SMF.1/Selection of the applied signature policy, FDP_ITC.2/Time reference, FPT_TDC.1/Time reference, FMT_MSA.3/Time reference, FMT_MSA.1/Time reference, FMT_MSA.1/Certificates, FMT_MSA.1/Certificates' validation data, FMT_SMR.1, FIA_UID.2	Section 7.2.1
O.Chemin_De_Certification	FDP_IFC.1/Certification path, FDP_ITC.2/Certification path, FPT_TDC.1/Certificates, FPT_TDC.1/Certificate revocation data, FMT_MTD.1/Selection of the applied signature policy, FMT_SMF.1/Selection of the applied signature policy, FMT_MSA.3/Certification path, FMT_MSA.1/Certificates, FMT_MSA.1/Certificates' validation data, FMT_SMR.1, FDP_IFF.1/Certification path, FIA_UID.2	Section 7.2.1

Objectifs de sécurité	Exigences fonctionnelles pour la TOE	Argumentaire
O.Conformité_Des_Certificats	FDP_IFC.1/Certification path, FDP_ITC.2/Certification path, FPT_TDC.1/Certificates, FPT_TDC.1/Certificate revocation data, FDP_IFF.1/Certification path, FMT_MTD.1/Selection of the applied signature policy, FMT_SMF.1/Selection of the applied signature policy, FMT_MSA.3/Certification path, FMT_MSA.1/Certificates, FMT_MSA.1/Certificates' validation data, FMT_SMR.1, FIA_UID.2	Section 7.2.1
O.Validité_Des_Certificats	FDP_IFC.1/Certification path, FDP_ITC.2/Certification path, FPT_TDC.1/Certificates, FPT_TDC.1/Certificate revocation data, FDP_IFF.1/Certification path, FMT_MTD.1/Selection of the applied signature policy, FMT_SMF.1/Selection of the applied signature policy, FMT_MSA.3/Certification path, FMT_MSA.1/Certificates, FMT_MSA.1/Certificates' validation data, FMT_SMR.1, FIA_UID.2	Section 7.2.1
O.Conformité_Données_Validation	FDP_IFC.1/Certification path, FDP_ITC.2/Certification path, FPT_TDC.1/Certificates, FPT_TDC.1/Certificate revocation data, FDP_IFF.1/Certification path, FMT_MTD.1/Selection of the applied signature policy, FMT_SMF.1/Selection of the applied signature policy, FMT_MSA.3/Certification path, FMT_MSA.1/Certificates, FMT_MSA.1/Certificates' validation data, FMT_SMR.1, FIA_UID.2	Section 7.2.1

Objectifs de sécurité	Exigences fonctionnelles pour la TOE	Argumentaire
O.Conformité_Attributs_Signés	FDP_IFC.1/Electronic signature, FDP_IFF.1/Electronic signature, FMT_MTD.1/Selection of the applied signature policy, FMT_SMF.1/Selection of the applied signature policy, FDP_ITC.2/Electronic signature, FPT_TDC.1/Electronic signature, FMT_MSA.3/Electronic signature, FMT_MSA.1/Electronic signature, FMT_SMR.1, FIA_UID.2	Section 7.2.1
O.Lancement_Applications_Présentation	FMT_MTD.1/Document format/viewer association table, FMT_MTD.1/Viewer activation parameter, FDP_IFF.1/Electronic signature, FMT_SMF.1/Management of the document format/viewer association table, FMT_SMF.1/Management of the viewer activation parameter	Section 7.2.1
O.Communication_Attributs_Signés	FDP_IFF.1/Electronic signature	Section 7.2.1
O.Export_Données_Validation	FDP_IFC.1/Electronic signature validation, FDP_IFF.1/Electronic signature validation, FDP_ETC.2/Verification status, FMT_MSA.3/Signature validation status, FMT_MSA.1/Signature validation status, FMT_SMR.1, FIA_UID.2	Section 7.2.1

Objectifs de sécurité	Exigences fonctionnelles pour la TOE	Argumentaire
O.Invocation_Module_Controle_Invariance	FDP_IFC.1/Document acceptance, FDP_IFF.1/Document acceptance, FDP_ITC.1/Document acceptance, FMT_MSA.3/Document's acceptance, FMT_MSA.1/Document's semantics invariance status, FMT_SMF.1/Getting document's semantics invariance status, FMT_SMR.1, FIA_UID.2	Section 7.2.1
O.Support_Cryptographique	FCS_COP.1/Signature verification, FCS_COP.1/Hash	Section 7.2.1

Tableau 6 Association objectifs de sécurité de la TOE vers les exigences fonctionnelles

Exigences fonctionnelles pour la TOE	Objectifs de sécurité
FDP_IFC.1/Document acceptance	O.Invocation_Module_Controle_Invariance
FDP_IFF.1/Document acceptance	O.Invocation_Module_Controle_Invariance
FDP_ITC.1/Document acceptance	O.Invocation_Module_Controle_Invariance
FMT_MSA.3/Document's acceptance	O.Invocation_Module_Controle_Invariance
FMT_MSA.1/Document's semantics invariance status	O.Invocation_Module_Controle_Invariance
FMT_SMF.1/Getting document's semantics invariance status	O.Invocation_Module_Controle_Invariance
FMT_MTD.1/Document format/viewer association table	O.Lancement_Applications_Présentation
FMT_SMF.1/Management of the document format/viewer association table	O.Administration, O.Lancement_Applications_Présentation
FMT_MTD.1/Viewer activation parameter	O.Lancement_Applications_Présentation
FMT_SMF.1/Management of the viewer activation parameter	O.Administration, O.Lancement_Applications_Présentation
FMT_MTD.1/Selection of the applied signature policy	O.Référence_De_Temps, O.Chemin_De_Certification, O.Conformité_Des_Certificats, O.Validité_Des_Certificats, O.Conformité_Données_Validation, O.Conformité_Attributs_Signés
FMT_SMF.1/Selection of the applied signature policy	O.Référence_De_Temps, O.Chemin_De_Certification, O.Conformité_Des_Certificats, O.Validité_Des_Certificats, O.Conformité_Données_Validation, O.Conformité_Attributs_Signés
FDP_IFC.1/Electronic signature	O.Conformité_Attributs_Signés

Exigences fonctionnelles pour la TOE	Objectifs de sécurité
FDP_IFF.1/Electronic signature	O.Conformité_Attributs_Signés, O.Lancement_Applications_Présentation, O.Communication_Attributs_Signés
FMT_MSA.3/Electronic signature	O.Conformité_Attributs_Signés
FMT_MSA.1/Electronic signature	O.Conformité_Attributs_Signés
FDP_ITC.2/Electronic signature	O.Conformité_Attributs_Signés
FDP_IFC.1/Time reference	O.Référence_De_Temps
FDP_IFF.1/Time reference	O.Référence_De_Temps
FMT_MSA.3/Time reference	O.Référence_De_Temps
FMT_MSA.1/Time reference	O.Référence_De_Temps
FDP_ITC.2/Time reference	O.Référence_De_Temps
FMT_MSA.1/Certificates	O.Référence_De_Temps, O.Chemin_De_Certification, O.Conformité_Des_Certificats, O.Validité_Des_Certificats, O.Conformité_Données_Validation
FMT_MSA.1/Certificates' validation data	O.Référence_De_Temps, O.Chemin_De_Certification, O.Conformité_Des_Certificats, O.Validité_Des_Certificats, O.Conformité_Données_Validation
FDP_IFC.1/Certification path	O.Chemin_De_Certification, O.Conformité_Des_Certificats, O.Validité_Des_Certificats, O.Conformité_Données_Validation
FDP_IFF.1/Certification path	O.Chemin_De_Certification, O.Conformité_Des_Certificats, O.Validité_Des_Certificats, O.Conformité_Données_Validation
FMT_MSA.3/Certification path	O.Chemin_De_Certification, O.Conformité_Des_Certificats, O.Validité_Des_Certificats, O.Conformité_Données_Validation

Exigences fonctionnelles pour la TOE	Objectifs de sécurité
FDP_ITC.2/Certification path	O.Chemin_De_Certification, O.Conformité_Des_Certificats, O.Validité_Des_Certificats, O.Conformité_Données_Validation
FPT_TDC.1/Electronic signature	O.Conformité_Attributs_Signés
FPT_TDC.1/Time reference	O.Référence_De_Temps
FPT_TDC.1/Certificates	O.Chemin_De_Certification, O.Conformité_Des_Certificats, O.Validité_Des_Certificats, O.Conformité_Données_Validation
FPT_TDC.1/Certificate revocation data	O.Chemin_De_Certification, O.Conformité_Des_Certificats, O.Validité_Des_Certificats, O.Conformité_Données_Validation
FDP_IFC.1/Electronic signature validation	O.Export_Données_Validation
FDP_IFF.1/Electronic signature validation	O.Export_Données_Validation
FMT_MSA.3/Signature validation status	O.Export_Données_Validation
FMT_MSA.1/Signature validation status	O.Export_Données_Validation
FDP_ETC.2/Verification status	O.Export_Données_Validation
FCS_COP.1/Signature verification	O.Support_Cryptographique
FCS_COP.1/Hash	O.Support_Cryptographique
FMT_SMR.1	O.Référence_De_Temps, O.Chemin_De_Certification, O.Conformité_Des_Certificats, O.Validité_Des_Certificats, O.Conformité_Données_Validation, O.Conformité_Attributs_Signés, O.Export_Données_Validation, O.Invocation_Module_Controle_Invariance

Exigences fonctionnelles pour la TOE	Objectifs de sécurité
FIA_UID.2	O.Référence_De_Temps, O.Chemin_De_Certification, O.Conformité_Des_Certificats, O.Validité_Des_Certificats, O.Conformité_Données_Validation, O.Conformité_Attributs_Signés, O.Export_Données_Validation, O.Invocation_Module_Controle_Invariance

Tableau 7 Association exigences fonctionnelles vers objectifs de sécurité de la TOE

7.3 Dépendances

7.3.1 Dépendances des exigences de sécurité fonctionnelles

Exigences	Dépendances CC	Dépendances Satisfaites
FDP_IFC.1/Document acceptance	(FDP_IFF.1)	FDP_IFF.1/Document acceptance
FDP_IFF.1/Document acceptance	(FDP_IFC.1) et (FMT_MSA.3)	FDP_IFC.1/Document acceptance, FMT_MSA.3/Document's acceptance
FDP_ITC.1/Document acceptance	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_MSA.3)	FDP_IFC.1/Document acceptance, FMT_MSA.3/Document's acceptance
FMT_MSA.3/Document's acceptance	(FMT_MSA.1) et (FMT_SMR.1)	FMT_MSA.1/Document's semantics invariance status, FMT_SMR.1
FMT_MSA.1/Document's semantics invariance status	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FDP_IFC.1/Document acceptance, FMT_SMF.1/Getting document's semantics invariance status, FMT_SMR.1
FMT_SMF.1/Getting document's semantics invariance status	Pas de dépendance	
FMT_MTD.1/Document format/viewer association table	(FMT_SMF.1) et (FMT_SMR.1)	FMT_SMF.1/Management of the document format/viewer association table, FMT_SMR.1
FMT_SMF.1/Management of the document format/viewer association table	Pas de dépendance	
FMT_MTD.1/Viewer activation parameter	(FMT_SMF.1) et (FMT_SMR.1)	FMT_SMF.1/Management of the viewer activation parameter, FMT_SMR.1
FMT_SMF.1/Management of the viewer activation parameter	Pas de dépendance	
FCS_COP.1/Signature verification	(FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2) et (FCS_CKM.4)	FDP_ITC.2/Certification path
FCS_COP.1/Hash	(FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2) et (FCS_CKM.4)	
FMT_SMR.1	(FIA_UID.1)	FIA_UID.2
FIA_UID.2	Pas de dépendance	
FMT_MTD.1/Selection of the applied signature policy	(FMT_SMF.1) et (FMT_SMR.1)	FMT_SMR.1, FMT_SMF.1/Selection of the applied signature policy

Exigences	Dépendances CC	Dépendances Satisfaites
FMT_SMF.1/Selection of the applied signature policy	Pas de dépendance	
FDP_IFC.1/Electronic signature	(FDP_IFF.1)	FDP_IFF.1/Electronic signature
FDP_IFF.1/Electronic signature	(FDP_IFC.1) et (FMT_MSA.3)	FDP_IFC.1/Electronic signature, FMT_MSA.3/Electronic signature
FMT_MSA.3/Electronic signature	(FMT_MSA.1) et (FMT_SMR.1)	FMT_SMR.1, FMT_MSA.1/Electronic signature
FMT_MSA.1/Electronic signature	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FMT_SMR.1, FDP_IFC.1/Electronic signature
FDP_ITC.2/Electronic signature	(FDP_ACC.1 ou FDP_IFC.1) et (FPT_TDC.1) et (FTP_ITC.1 ou FTP_TRP.1)	FDP_IFC.1/Electronic signature, FPT_TDC.1/Electronic signature
FDP_IFC.1/Time reference	(FDP_IFF.1)	FDP_IFF.1/Time reference
FDP_IFF.1/Time reference	(FDP_IFC.1) et (FMT_MSA.3)	FDP_IFC.1/Time reference, FMT_MSA.3/Time reference
FMT_MSA.3/Time reference	(FMT_MSA.1) et (FMT_SMR.1)	FMT_SMR.1, FMT_MSA.1/Time reference, FMT_MSA.1/Certificates, FMT_MSA.1/Certificates' validation data
FMT_MSA.1/Time reference	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FMT_SMR.1, FDP_IFC.1/Time reference
FDP_ITC.2/Time reference	(FDP_ACC.1 ou FDP_IFC.1) et (FPT_TDC.1) et (FTP_ITC.1 ou FTP_TRP.1)	FDP_IFC.1/Time reference, FPT_TDC.1/Time reference, FPT_TDC.1/Certificates, FPT_TDC.1/Certificate revocation data
FDP_IFC.1/Certification path	(FDP_IFF.1)	FDP_IFF.1/Certification path
FDP_IFF.1/Certification path	(FDP_IFC.1) et (FMT_MSA.3)	FDP_IFC.1/Certification path, FMT_MSA.3/Certification path
FMT_MSA.3/Certification path	(FMT_MSA.1) et (FMT_SMR.1)	FMT_SMR.1, FMT_MSA.1/Certificates, FMT_MSA.1/Certificates' validation data

Exigences	Dépendances CC	Dépendances Satisfaites
FDP_ITC.2/Certification path	(FDP_ACC.1 ou FDP_IFC.1) et (FPT_TDC.1) et (FTP_ITC.1 ou FTP_TRP.1)	FDP_IFC.1/Certification path, FPT_TDC.1/Certificates, FPT_TDC.1/Certificate revocation data
FPT_TDC.1/Electronic signature	Pas de dépendance	
FPT_TDC.1/Time reference	Pas de dépendance	
FPT_TDC.1/Certificates	Pas de dépendance	
FPT_TDC.1/Certificate revocation data	Pas de dépendance	
FDP_IFC.1/Electronic signature validation	(FDP_IFF.1)	FDP_IFF.1/Electronic signature validation
FDP_IFF.1/Electronic signature validation	(FDP_IFC.1) et (FMT_MSA.3)	FDP_IFC.1/Electronic signature validation, FMT_MSA.3/Signature validation status
FMT_MSA.3/Signature validation status	(FMT_MSA.1) et (FMT_SMR.1)	FMT_SMR.1, FMT_MSA.1/Signature validation status
FMT_MSA.1/Signature validation status	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FMT_SMR.1, FDP_IFC.1/Electronic signature validation
FDP_ETC.2/Verification status	(FDP_ACC.1 ou FDP_IFC.1)	FDP_IFC.1/Electronic signature validation
FMT_MSA.1/Certificates	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FMT_SMR.1, FDP_IFC.1/Certification path
FMT_MSA.1/Certificates' validation data	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FMT_SMR.1, FDP_IFC.1/Certification path

Tableau 8 Dépendances des exigences fonctionnelles

7.3.1.1 Argumentaire pour les dépendances non satisfaites

La dépendance FCS_CKM.4 de FCS_COP.1/Signature verification n'est pas supportée. La dépendance entre *FCS_COP.1/Signature verification* et *FCS_CKM.4* n'est pas satisfaite, puisque les clés utilisées étant des clés publiques elles ne nécessitent pas de méthode sécurisée pour leur destruction.

La dépendance FCS_CKM.4 de FCS_COP.1/Hash n'est pas supportée. La dépendance entre le composant *FCS_COP.1/Hash* et le composant *FCS_CKM.4* n'est pas

satisfaite car un algorithme de hachage ne nécessite pas de clé, donc ne requiert pas d'exigences décrivant les méthodes de destruction des clés.

La dépendance FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 de FCS_COP.1/Hash n'est pas supportée. La dépendance entre le composant FCS_COP.1/Hash et un des trois composants FCS_CKM.1, FDP_ITC.1 et FDP_ITC.2 n'est pas satisfaite car un algorithme de hachage ne nécessite pas de clé, donc ne requiert pas d'exigences décrivant les méthodes de génération ou d'import de clés

La dépendance FMT_SMF.1 de FMT_MSA.1/Electronic signature n'est pas supportée. Le composant *FMT_MSA.1/Electronic signature* ne définissant pas de nouvelle fonctionnalité de gestion, la dépendance entre ce composant et le composant *FMT_SMF.1* n'a pas besoin d'être satisfaite.

La dépendance FTP_ITC.1 or FTP_TRP.1 de FDP_ITC.2/Electronic signature n'est pas supportée. La dépendance entre le composant d'exigence *FDP_ITC.2/Electronic signature* et un des composant FTP_ITC.1 ou TFP_TRP.1 n'est pas satisfaite car:

- ces données ne nécessitent pas de protection en confidentialité;
- la validité de la signature numérique contenue dans la signature électronique garantit l'intégrité des toutes les données signées;
- enfin, la validité de la signature électronique (si elle est attestée à la fin du processus de vérification) prouve l'authenticité de l'origine de l'information.

La dépendance FMT_SMF.1 de FMT_MSA.1/Time reference n'est pas supportée. La dépendance entre le composant *FMT_MSA.1/Time reference* et le composant FMT_SMF.1 n'est pas satisfaite car ce premier composant ne définit pas de nouvelle fonction de gestion des attributs de sécurité.

La dépendance FTP_ITC.1 or FTP_TRP.1 de FDP_ITC.2/Time reference n'est pas supportée. La dépendance entre le composant d'exigence *FDP_ITC.2/Certificates' validation data* et un des composants FTP_ITC.1 ou FTP_TRP.1 n'a pas à être satisfaite car les données véhiculées par les protocoles utilisés dans les infrastructures à clé publique sont autoprotégées:

- l'intégrité de la référence de temps est garantie par la signature numérique qui lui est associée;
- l'authenticité de l'origine de la référence de temps est garantie par la construction d'un chemin de certification valide entre la clé de l'unité d'horodatage et un point de confiance dédié à l'horodatage défini dans la politique de signature.
- enfin, les données reçues par la TOE ne nécessitent pas de protection en termes de confidentialité.

La dépendance FTP_ITC.1 or FTP_TRP.1 de FDP_ITC.2/Certification path n'est pas supportée. La dépendance entre le composant d'exigence *FDP_ITC.2/Certification path* et un des composant FTP_ITC.1 ou FTP_TRP.1 n'a pas à être satisfaite car les protocoles utilisés dans les infrastructures à clé publiques sont autoprotégés:

- l'intégrité de chacun des certificats de la chaîne de certification et des informations de non révocation est garantie par une signature numérique apposée par une

autorité supérieure, le certificat autosigné racine étant référencé dans la politique de signature (protégée en intégrité par la TOE).

- le fait de construire une chaîne de certification valide entre le certificat du signataire et un point de confiance défini dans la politique de signature permet à lui seul de garantir l'authenticité de l'origine des différents certificats composant cette chaîne.
- les données reçues par la TOE ne nécessitent pas de protection en termes de confidentialité.

La dépendance FMT_SMF.1 de FMT_MSA.1/Signature validation status n'est pas supportée. La dépendance entre le composant *FMT_MSA.1/Signature validation status* et le composant FMT_SMF.1 n'est pas satisfaite car ce premier composant ne définit pas de nouvelle fonction de gestion des attributs de sécurité.

La dépendance FMT_SMF.1 de FMT_MSA.1/Certificates n'est pas supportée. Le composant *FMT_MSA.1/Certificated* ne définissant pas de nouvelle fonctionnalité de gestion, la dépendance entre ce composant et le composant *FMT_SMF.1* n'a pas besoin d'être satisfaite.

La dépendance FMT_SMF.1 de FMT_MSA.1/Certificates' validation data n'est pas supportée. Le composant *FMT_MSA.1/Certificates' validation data* ne définissant pas de nouvelle fonctionnalité de gestion, la dépendance entre ce composant et le composant *FMT_SMF.1* n'a pas besoin d'être satisfaite.

7.3.2 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

Exigences	Dépendances CC	Dépendances Satisfaites
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.3	(ADV_ARC.1) et (ADV_FSP.2) et (ADV_IMP.1) et (ADV_TDS.3) et (AGD_OPE.1) et (AGD_PRE.1)	ADV_ARC.1, ADV_FSP.3, AGD_OPE.1, AGD_PRE.1

Tableau 9 Dépendances des exigences d'assurance

7.3.2.1 Argumentaire pour les dépendances non satisfaites

La dépendance ADV_IMP.1 de AVA_VAN.3 n'est pas supportée. La dépendance avec ADV_IMP.1 n'est pas satisfaite car cette exigence est couverte par le composant d'exigence AVA_VAN.3.

La dépendance ADV_TDS.3 de AVA_VAN.3 n'est pas supportée. La dépendance avec ADV_TDS.3 n'est pas satisfaite car cette exigence est couverte par le composant d'exigence AVA_VAN.3.

7.4 Argumentaire pour l'EAL

Le niveau d'assurance de ce profil de protection est EAL3 augmenté, car il est requis par le processus de qualification standard [QUA-STD].

7.5 Argumentaire pour les augmentations à l'EAL

7.5.1 ALC_FLR.3 Systematic flaw remediation

Augmentation requise par le processus de qualification standard.

7.5.2 AVA_VAN.3 Focused vulnerability analysis

Augmentation requise par le processus de qualification standard.

8 Notice

Ce document a été généré avec TL SET version 2.2.8 (for CC3). Pour plus d'informations sur l'outil d'édition sécuritaire de Trusted Labs consultez le site internet www.trusted-labs.com.

Annexe A Glossaire

Ce glossaire donne la définition de termes utilisés dans le reste de ce document ; ces termes sont soulignés lors de leur première apparition dans le texte.

Le glossaire est composé de deux parties. La première partie est relative aux termes spécifiques au Critères Communs, la seconde explicite les termes relatifs au domaine de la signature électronique.

A.1 Termes propres aux Critères Communs

Evaluation Assurance Level (EAL)

Un paquet constitué d'exigences d'assurance tirées de la partie 3 qui représente un point sur l'échelle d'assurance prédéfinie dans les Critères Communs.

Target Of Evaluation (TOE)

En français, Cible d'évaluation.

Un produit ou un système de traitement d'informations ainsi que sa documentation d'administration et d'utilisation qui est le sujet de l'évaluation.

TOE Security Policy (TSP)

En français, politique de sécurité de la TOE.

Un ensemble de règles qui réglemente comment des biens sont gérés, protégés et distribuée à l'intérieur d'une cible d'évaluation.

A.2 Termes propres à la signature électronique

Autorité de certification qualifiée

Entité fournissant des certificats remplissant les conditions définies à l'annexe II de la Directive

Certificat électronique

Un document sous forme électronique attestant du lien entre les *données de vérification de signature électronique* et un *signataire*.

Un certificat électronique doit comporter :

a) L'identité du prestataire de services de certification électronique ainsi que l'État dans lequel il est établi ;

b) Le nom du signataire ou un pseudonyme, celui-ci devant alors être identifié comme tel ;

c) Le cas échéant, l'indication de la qualité du signataire en fonction de l'usage auquel le certificat électronique est destiné ;

d) Les données de vérification de signature électronique qui correspondent aux données de création de signature électronique ;

e) L'indication du début et de la fin de la période de validité du certificat électronique ;

f) Le code d'identité du certificat électronique ;

g) La signature électronique du prestataire de services de certification électronique qui délivre le certificat électronique ;

Le cas échéant, les conditions d'utilisation du certificat électronique, notamment le montant maximum des transactions pour lesquelles ce certificat peut être utilisé.

Certificat électronique qualifié

Un *certificat électronique* répondant aux exigences définies à l'article 6 du Décret no 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique.

C'est à dire, en sus des éléments définis ci-dessus, un certificat électronique qualifié doit comporter :

a) Une mention indiquant que ce certificat est délivré à titre de certificat électronique qualifié ;

b) La signature électronique *sécurisée* du prestataire de services de certification électronique qui délivre le certificat électronique.

Condensé

Résultat d'une fonction de hachage à sens unique, c'est-à-dire d'une fonction calculant une empreinte d'un message de telle sorte qu'une modification même infime du message entraîne la modification de l'empreinte. En français, on utilise encore les termes « haché » et « condensé ». Le terme anglais équivalent est « hash value ».

Cryptographic Service Provider (CSP)

En français, fournisseur de services cryptographiques.

Couche logicielle permettant à une application d'utiliser des services cryptographiques grâce à une interface programmatique (API) bien définie fournie par le système d'exploitation de la machine hôte.

Dispositif de création de signature électronique

Un matériel ou un logiciel destiné à mettre en application les *données de création de signature électronique* pour générer des signature électroniques. Acronyme anglais SCDev pour *signature creation device*.

Dispositif sécurisé de création de signature électronique

Un *dispositif de création de signature électronique* qui satisfait aux exigences définies au I de l'article 3 du Décret no 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique. Acronyme anglais SSCD pour *secure signature creation device*.

Dispositif de vérification de signature électronique

Un matériel ou un logiciel destiné à mettre en application *les données de vérification de signature électronique*.

Directive

Directive 1999/93/EC du parlement européen et du conseil du 13 décembre 1999 pour un cadre communautaire sur la signature électronique.

Données de création de signature électronique

Les éléments propres au *signataire*, tels que des clés cryptographiques privées, utilisés par lui pour créer une *signature électronique* ;

Données de vérification de signature électronique

Les éléments, tels que des clés cryptographiques publiques, utilisés pour vérifier la *signature électronique*.

Format de contenu

Un identifiant permettant de déterminer le type d'application capable de présenter correctement le document.

Object Identifier (OID)

Suite de caractères numériques ou alphanumériques, enregistrés in conformément à la norme ISO/IEC 9834, qui identifient de manière unique un objet ou une classe d'objets dans l'enveloppe d'une signature électronique.

Politique de signature

Ensemble de règles pour la création ou la validation d'une signature électronique, sous lesquelles une signature peut être déterminée valide.

Prestataire de services de certification électronique

Toute personne qui délivre des *certificats électroniques* ou fournit d'autres services en matière de *signature électronique*.

Qualification des prestataires de services de certification électronique

L'acte par lequel un tiers, dit organisme de qualification, atteste qu'un *prestataire de services de certification électronique* fournit des prestations conformes à des exigences particulières de qualité.

Signataire

Toute personne physique, agissant pour son propre compte ou pour celui de la personne physique ou morale qu'elle représente, qui met en oeuvre un *dispositif de création de signature électronique* ;

Signature électronique

Donnée sous forme électronique, jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification pour ces données électroniques.

Signature électronique sécurisée

Une *signature électronique* qui satisfait, en outre, aux exigences suivantes :

- être propre au signataire ;
- être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ;
- garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable ;

Signature électronique présumée fiable

Une signature mettant en œuvre une signature électronique sécurisée, établie grâce à un dispositif sécurisé de création de signature électronique et reposant sur l'utilisation d'un certificat électronique qualifié.

On parle aussi de signature électronique qualifiée.

Signature numérique

Résultat de l'opération cryptographique de signature sur des données à signer et utilisant une clé privée de signature.

Système de création de signature

Le système complet qui permet la création d'une signature électronique et qui inclut l'application de création de signature et le dispositif de création de signature.

Annexe B Acronymes

ETSI European Telecommunications Standards Institute

CWA CEN Workshop Agreements

CSP Cryptographic Service Provider.

TOE Target of Evaluation, en français, cible d'évaluation

SCDev Signature Creation Device

SSCD Secure Signature Creation Device

OID Object Identifier, en français identifiant d'objet.

Index

B

B.Attributs_Signés 20
B.Correspondance_Données_Internes/Externes .. 22
B.Correspondance_FormatDoc_Application 22
B.Document 20
B.Données_A_Vérifier___Hachées 21
B.Données_De_Validation_En_Entrée..... 20
B.Données_De_Validation_En_Sortie..... 21
B.Politiques_De_Signature 22
B.Règles_De_Vérification 22
B.Services 21
B.Signature..... 20
B.Statut_De_Retour 21

F

FCS_COP.1/Hash 48
FCS_COP.1/Signature__verification 48
FDP_ETC.2/Verification__status 47
FDP_IFC.1/Certification__path 41
FDP_IFC.1/Document__acceptance 33
FDP_IFC.1/Electronic__signature 36
FDP_IFC.1/Electronic__signature__validation ... 46
FDP_IFC.1/Time__reference..... 39
FDP_IFF.1/Certification__path 42
FDP_IFF.1/Document__acceptance 33
FDP_IFF.1/Electronic__signature..... 37
FDP_IFF.1/Electronic__signature__validation.... 46
FDP_IFF.1/Time__reference 39
FDP_ITC.1/Document__acceptance..... 34
FDP_ITC.2/Certification__path..... 43
FDP_ITC.2/Electronic__signature..... 38
FDP_ITC.2/Time__reference..... 40
FIA_UID.2 48
FMT_MSA.1/Certificates 41
FMT_MSA.1/Certificates'__validation__data 41
FMT_MSA.1/Document's__semantics__invariance __status 35
FMT_MSA.1/Electronic__signature..... 38
FMT_MSA.1/Signature__validation__status..... 47
FMT_MSA.1/Time__reference 40
FMT_MSA.3/Certification__path..... 43
FMT_MSA.3/Document's__acceptance 34
FMT_MSA.3/Electronic__signature..... 38
FMT_MSA.3/Signature__validation__status..... 46
FMT_MSA.3/Time__reference 40
FMT_MTD.1/Document__format/viewer__associat ion__table..... 35
FMT_MTD.1/Selection__of__the__applied__signa ture__policy 36
FMT_MTD.1/Viewer__activation__parameter ... 35
FMT_SMF.1/Getting__document's__semantics__in variance__status 35
FMT_SMF.1/Management__of__the__document__ format/viewer__association__table..... 35
FMT_SMF.1/Management__of__the__viewer__act ivation__parameter 36
FMT_SMF.1/Selection__of__the__applied__signat ure__policy 36
FMT_SMR.1..... 48
FPT_TDC.1/Certificate__revocation__data 45
FPT_TDC.1/Certificates 45
FPT_TDC.1/Electronic__signature..... 44
FPT_TDC.1/Time__reference 44

H

H.Accès_Données_De_Validation 26
H.Administrateur_De_Sécurité_Sûr 26
H.Contrôle_Invariance_Sémantique_Document.. 26
H.Intégrité_Services..... 26
H.Machine_Hôte..... 25
H.Politique_Signature_D'Origine_Authentique... 25
H.Présentation_Document 26

O

O.Administration 27
O.Chemin_De_Certification 27
O.Communication_Attributs_Signés 28
O.Conformité_Attributs_Signés 28
O.Conformité_Des_Certificats 27
O.Conformité_Données_Validation 28
O.Export_Données_Validation..... 28
O.Invocation_Module_Controle_Invariance..... 28
O.Lancement_Applications_Présentation..... 28
O.Référence_De_Temps..... 27
O.Support_Cryptographique..... 29
O.Validité_Des_Certificats..... 27
OE.Administrateur_De_Sécurité_Sûr..... 30
OE.Authenticité_Origine_Politique_Signature.... 29
OE.Contrôle_Sémantique_Document_Signé..... 30
OE.Fourniture_Des_Données_De_Validation..... 30
OE.Intégrité_Services 30
OE.Machine_Hôte 29
OE.Présentation_Document..... 29

P

P.Administration 25
P.Algorithmes_De_Hachage..... 24
P.Algorithmes_De_Signature 24
P.Authenticité/Intégrité_Données_Validation 24
P.Authenticité_Certificat_Signataire 24
P.Communication_Attributs_Signés..... 24
P.Conformité_Attributs_Signés 23
P.Conformité_Certificat_Signataire..... 23
P.Export_Données_Validation..... 25
P.Possibilité_Présenter_Document 24
P.Sémantique_Document_Invariante..... 24
P.Validité_Certificat_Signataire 23

S

S.Administrateur_De_Sécurité 23
S.Vérificateur..... 23