Date : 01 Juin 2010

Origine : DES/SEC

Dossier : *TRUSTYSIGN V4*

Titre :

CIBLE DE SÉCURITÉ CRITÈRES COMMUNS TRUSTYSIGN V4

Référence : CSSI/HLS/TRUSTY/FR/7/0057-2.0

État :

TABLE DES MATIÈRES

Références

[CC]	Common Criteria for Information Technology Security Evaluation, version 3.1 – Part 1: Introduction and general model revision 1, ref. CCMB-2006-09-001 – Part 2: Security functional requirements revision 2, ref. CCMB-2007-09-002 – Part 3: Security assurance requirements revision 2, ref. CCMB-2007-09-003
[DCSSI_CRYPTO]	Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard, Version 1.11 du 24 Octobre 2008
[DCSSI_GESTION_CLES]	Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques de niveau de robustesse standard, Version 1.10 du 24 Octobre 2008
[Directive]	Directive européenne sur la signature électronique, 13 décembre 1999, 1999/93/CE.
[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.
[PP2008/06]	Profil de protection – Module de vérification de signature version 1.6, réf PP-MVSE-CCv3.1, DCSSI
[PP2008/05]	Profil de protection – Application de création de signature électronique version 1.6, réf PP-ACSE-CCv3.1, DCSSI

Glossaire

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

1 Introduction

1.1 Identification de la cible de sécurité (ST)

Titre	Cible de Sécurité Critères Communs TrustySign V4 : CSSI/HLS/TRUSTY/FR/7/0057-2.0
Version	2.0
Auteur(s)	Christophe BLAD/Frédéric CARO
Date	01/06/2010

1.2 Identification de la cible d'évaluation (TOE)

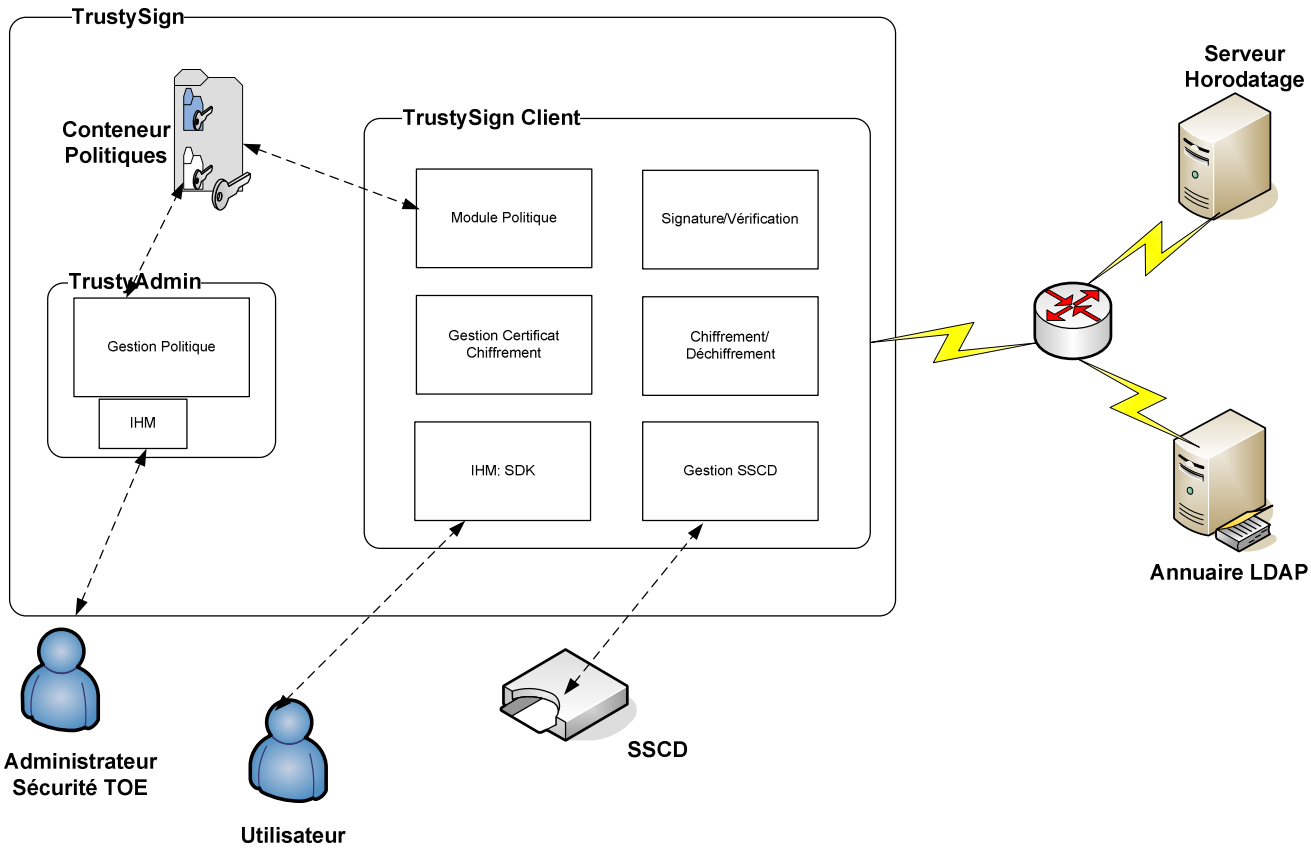
Développeur	CS Communications
Nom du produit	TrustySign
Version	4.1.4
Plateforme cible	Système d'exploitation Microsoft Windows Vista SP1, token Oberthur ID-ONE

1.3 Vue d'ensemble de la cible d'évaluation

TrustySign V4 est une application destinée aux communautés d'utilisateurs (entreprises, corporations professionnelles, places de marché B-to-B) permettant de chiffrer et de signer des fichiers à l'aide de clés privées stockées sur carte à puce ou support logiciel.

TrustySign V4 dispose également d'une fonction d'administration locale des certificats (pour les besoins de chiffrement). Par ailleurs, TrustySign V4 s'interface avec les clients de messagerie standards ; les documents chiffrés/signés pouvant être envoyés en tant que pièce jointe.

Enfin TrustySign dispose d'une composante d'administration (TrustyAdmin) permettant de gérer les politiques de signature et de chiffrement assurant le pilotage des opérations de sécurité.



1.4 Description de la cible d'évaluation

La cible d'évaluation (TOE) est un ensemble de composants logiciels permettant à la fois :

- de créer des signatures électroniques en s'appuyant sur un dispositif de création de signature (dénommé par la suite SCDev) effectuant les calculs cryptographiques mettant en oeuvre la clé privée du signataire,
- de vérifier une signature électronique d'un document,
- de chiffrer/déchiffrer un document pour un ou plusieurs destinataires,
- de gérer les politiques de signature et de chiffrement applicables aux opérations de sécurité,
- d'administrer et de configurer la TOE.

Ces fonctionnalités sont accessibles soit via une IHM TrustySign (mode manuel), soit via une API (mode SDK).

Les services suivants ne font pas partie du périmètre de l'évaluation :

- Communication (envoi des fichiers signés, chiffrés,..) au destinataire via l'interface MAPI.
- Visualisation.

1.4.1 Description des services fournis par la TOE

Signature d'un document (TrustySign Client)

Le service de signature offre la possibilité de signer un ou des fichiers sous divers format :

- Format de signature CMS :
  - ❖ Mise en œuvre des co-signatures et sur-signatures.
  - ❖ Implémentation format étendu CAdES.
  - ❖ Mode de Signature CMS attaché au document.
  - ❖ Algorithmes Cryptographiques supportés :
    - RSA (1024 ou 2048 bits) avec SHA512.
    - RSA (1024 ou 2048 bits) avec SHA-384.
    - RSA (1024 ou 2048 bits) avec SHA-256.
    - RSA (1024 ou 2048 bits) avec SHA-1.
- Format de signature XML
  - ❖ XML/DSIG.
  - ❖ XAdES (format 1.2.2 et 1.3.2).
  - ❖ Implémentation de la Signature Enveloppée XML (signature unique ou multi-signature au sein du document XML).
  - ❖ Implémentation de la signature enveloppante XML.
  - ❖ Algorithmes Cryptographiques supportés :
    - RSA (1024 ou 2048 bits) avec SHA512.
    - RSA (1024 ou 2048 bits) avec SHA-384.
    - RSA (1024 ou 2048 bits) avec SHA-256.
    - RSA (1024 ou 2048 bits) avec SHA-1.

Cette signature s'effectue selon la politique de signature sélectionnée par le signataire, permettant par exemple la validation du certificat signataire et/ou pour les formats CMS et XADES d'effectuer une requête pour récupérer un tampon d'horodatage.

Vérification de signature (TrustySign Client)

Le service de vérification de signature offre la possibilité de vérifier la signature de fichiers sous divers format :

- CMS en signature, sur signature ou co-signature.
- XML pour une signature XML/XADES ou XML/DSIG.

Il réalise selon la politique de signature, la vérification de la chaîne de certification pour les certificats utilisés pour la signature et pour les formats CMS et XADES la vérification des tampons d'horodatages pouvant être présents dans les données à vérifier.
Par ailleurs, ce service assure l'extraction du document d'origine dans le cas du format CMS.
Il présente un rapport de vérification avec les attributs du document d'origine et de la signature.

Chiffrement d'un document (TrustySign Client)

Le service de chiffrement offre la possibilité de chiffrer des fichiers sous divers format pour un ou plusieurs destinataires :

- CMS en chiffrement.
- XML pour un chiffrement XMLEnc.
- Algorithmes Supportés :
  - o AES-128
  - o AES-192
  - o AES-256

Il peut selon la politique de chiffrement, vérifier ou non la validité du certificat des destinataires avant le chiffrement.

Déchiffrement d'un document (TrustySign Client)
Le service de déchiffrement offre la possibilité de déchiffrer un fichier sous divers format :

- CMS en chiffrement.
- XML pour un chiffrement XMLEnc.

Gestion des politiques (TrustySign Client)
Ce service assure la gestion des politiques de signature/chiffrement. Il réalise les opérations suivantes :

- Lecture des "fichiers" politiques, les "fichiers" de politiques sont stockés dans un seul fichier de configuration signé de TrustySign. L'accès aux politiques nécessite la vérification de ce fichier de configuration.
- Stockage des objets de politiques.
- Recherche d'un objet de politique sur la demande des autres services.[2]
- Vérification de la cohérence sémantique du fichier de politique.
- Le TrustySign V4 n'administre pas directement les politiques, il utilise une configuration contenant les fichiers de politique..

La politique de signature est décrite dans un fichier au format XML. Ce fichier est signé.

Un profil décrit dans la politique peut contenir les informations suivantes :

- Algorithme de Hashage.
- Algorithme de canonicalisation (cas de la signature XML).
- Référence de la politique de signature.
- L'autorisation de poursuivre ou pas le processus en cas d'instabilité sémantique du document.
- La liste des formats de document à signer autorisée, les applications de présentation externes correspondantes et les modules de stabilité correspondants à invoquer.
- Types d'engagement autorisés.
- Rôles du signataire autorisés.
- Dans le cas d'un document XML, des références de nœud sur lesquelles doit porter la signature.
- Règle de demande d'un jeton d'horodatage (listes de serveurs d'horodatage consultables, demande de récupération du certificat d'horodatage et règles de validation de ce certificat, OID de politique d'horodatage autorisé).
- Règles de validation et de construction de la chaîne de certification du certificat signataire (liste des AC autorisées, liste des annuaires LDAP consultables, demande d'utilisation des CRL et/ou des CRL distribution point dans la validation de la chaîne de certification, utilisation serveur OCSP).
- Règle de contrôle de certaines extensions sur le certificat signataire.

Pour les opérations de chiffrement/déchiffrement, cette fonction génère un profil pouvant contenir les informations suivantes :

- Algorithme de chiffrement symétrique utilisé
- Règles de validation et de construction de la chaîne de certification du certificat de chiffrement destinataire (liste des AC autorisées, liste des annuaires LDAP consultables, demande d'utilisation des CRL et/ou des CRL distribution point dans la validation de la chaîne de certification, utilisation serveur OCSP).

- Règle de contrôle de certaines extensions sur le certificat de chiffrement destinataire

Administration/configuration (TrustySign Client)
Le service d'administration et de configuration offre plusieurs fonctionnalités :

- Gestion de la configuration utilisateur (gestion du support d'identification, choix des librairies PKCS#11 et test de connectivité avec le support de certificat)
- Présentation des résultats d'une vérification de signature
- Intégration au menu contextuel du Système d'exploitation
- Affichage de la fenêtre d'identification
- Journalisation des opérations

Administration des Politiques (TrustyAdmin)
Ce service est dédié à l'administrateur de sécurité de la TOE.

Le service d'administration des politiques permet via une IHM:

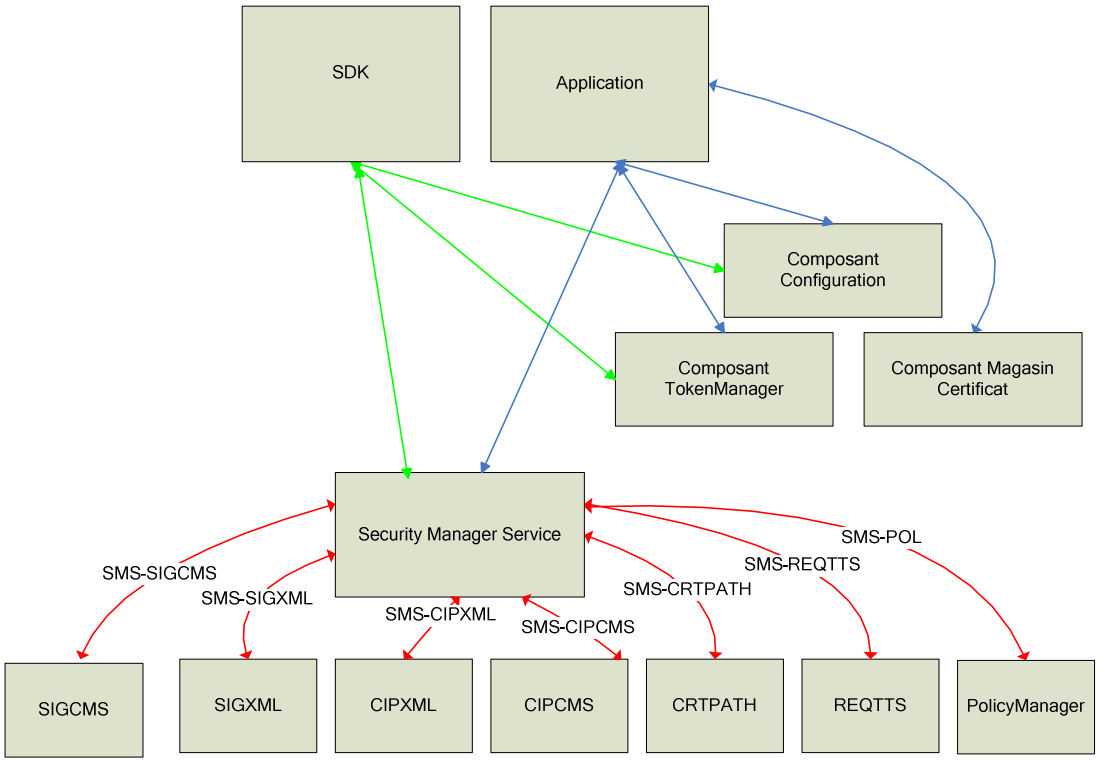
- Gestion des politiques de signature applicable à TrustySign Client (ajout/suppression/visualisation)
- Gestion des politiques de chiffrement à TrustySign Client (ajout/suppression/visualisation)
- Authentification préalable de l'administrateur TOE

1.4.2 Architecture de la TOE

TrustySign est constitué d'une architecture logicielle présentant :

- Un niveau composant de sécurité piloté par un Security Manager Service qui constitue le cœur de la couche sécurité ;
- Un ensemble de composants de sécurité réalisant les opérations unitaires de signature, vérification, chiffrement, déchiffrement, validation de certificat, demande de tampon d'horodatage
- Un niveau composant administratif permettant de fournir les services utiles aux opérations de sécurité. Ces composants sont configurables par l'utilisateur à travers des paramètres de configuration ou à travers des IHM (dans le cas du gestionnaire de certificat de chiffrement) décrits par la suite ;
- Un niveau applicatif qui se présente sous deux formes différentes :
  - Pour le SDK, il est constitué de classes Java permettant d'appeler les services des composants de sécurité.
  - Pour l'applicatif TrustySign, il se présente sous la forme d'IHM permettant d'invoquer les services des composants de sécurité ou des composants administratifs.

Cette architecture peut être représentée sous la forme suivante :



1.4.3 Environnement d'utilisation de la TOE

L'application s'intègre sur une plate-forme hôte (un ordinateur personnel, une borne publique, un organiseur personnel, …).

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

- Le système d'exploitation de la machine hôte
- Les composants logiciel installés sur le système d'exploitation permettant de communiquer avec le SCDev pour les fonctionnalités de signature (ex : les pilotes PKCS#11 ou des fournisseurs de services cryptographiques (CSP) définissant une interface cryptographique que l'application de signature appelle pour accéder à un module générant effectivement la signature). Pour la fonctionnalité de déchiffrement, la TOE s'appuie sur le Keystore géré par l'environnement Java pour accéder au bi-clé de l'utilisateur. Le Keystore géré est soit un SSCD ou un PKCS#12.
- Un SCDev électronique (SCDev) (tel qu'une carte à microcircuit, un token USB, ou un composant logiciel implanté dans la plate-forme hôte elle-même).

Du fait de la technologie employée (application Java), l'application TrustySign peut être utilisée sur n'importe quel système d'exploitation embarquant un environnement JRE 5. Le système d'exploitation retenu pour cette évaluation est Windows Vista SP1

Pour l'évaluation, les tests sont effectués sur un système d'exploitation Windows Vista SP1 et avec un token Oberthur ID-ONE.

Affichage des documents

Le logiciel permettant de présenter le document et 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, …) n'entre pas dans le périmètre de la TOE.

Edition des fichiers de politiques

L'édition et la signature des fichiers contenant les politiques de signature/chiffrement sont réalisées par l'Administrateur de Sécurité à l'aide d'une application qui n'entre pas dans le périmètre de la TOE.

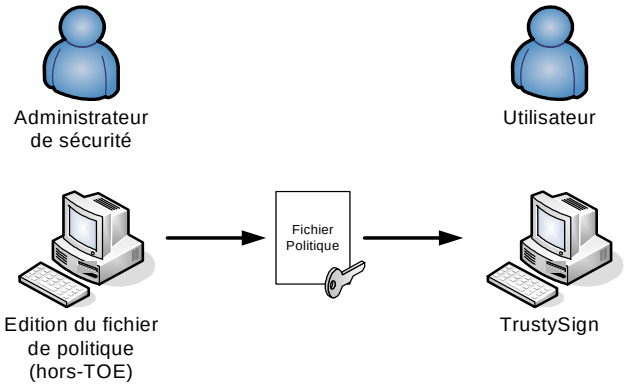


Figure 1 Edition du fichier de politiques

2 Déclaration de conformité

2.1 Conformité aux Critères communs

Cette cible de sécurité est **strictement conforme** aux parties 2et 3 des Critères Communs [CC] version 3.1 révision 2.

2.2 Conformité à un profil de protection

Cette cible de sécurité n'est conforme à aucun profil de protection mais s'inspire largement des exigences à la fois au profil de protection « Application de création de signature électronique », réf. PP-ACSE-CCv3.1 v1.6 [PP2008/05], et du profil de protection « module de vérification de signature électronique », réf. PP-MVSE-CCv3.1 v1.6 [PP2008/06].

2.3 Conformité à un paquet d'assurance

Le niveau visé est **EAL3 augmenté** du composant ALC_FLR.3. Ce paquet d'assurance permet de garantir, par une analyse indépendante, que la TOE satisfait les exigences requises:

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

3 Définition du problème de sécurité

3.1 Biens à protéger

3.1.1 Biens à protéger par la TOE

Cette section présente les biens de l'utilisateur qui doivent être protégés par la TOE. Ces données ne doivent pas pouvoir être modifiées de manière illicite lors de leur traitement.

3.1.1.1 Données en entrée

B.Documents_A_Signer/Chiffrer/Déchiffrer
L'ensemble des documents à signer, à chiffrer ou à déchiffrer peut être composé de:

- soit un unique document électronique.
- soit plusieurs documents électroniques.

B.Document_A_Vérifier
Le document à vérifier est un document signé et pour lequel la TOE doit vérifier la signature. Il peut être fourni à la TOE soit dans le même fichier que sa signature soit dans un fichier indépendant.

3.1.1.2 Données retournées par la TOE

B.Document_Chiffré
Documents après les opérations de chiffrement.

B.Document_EnClair
Documents après les opérations de déchiffrement.

B.Signature_Electronique
La signature électronique est une enveloppe comprenant:

- Le condensé de l'ensemble des données à signer;
- La signature numérique;
- Des informations supplémentaires pouvant faciliter la vérification de signature.

Ce bien doit être protégé par la TOE au cours de sa constitution avant qu'il soit transmis au signataire.

B.Statut_De_Retour
Après une 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.

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.

3.1.2 Biens sensibles de la TOE

Cette section présente les biens propres de la TOE qui sont mis en jeu dans le cadre des opérations de la TOE.

B.Services
Ce bien représente le code exécutable implémentant les services rendus. Le code de la TOE doit être protégé en intégrité.

B.Politiques
Les politiques de signature et de chiffrement définissent les règles à appliquer pour signer, pour vérifier une signature donnée ou pour chiffrer/déchiffrer les documents.
La TOE supporte une ou plusieurs politiques de signature/chiffrement. La liste des politiques, qui est gérée par l'administrateur de la TOE, doit être protégée en intégrité. De plus, l'intégrité de chacune des politiques de signature doit aussi être contrôlée.

B.Clés_Chiffrement/Déchiffrement
Les clés cryptographiques utilisées pour le chiffrement/déchiffrement des documents doivent être protégées en confidentialité et en intégrité. Le mécanisme de chiffrement/déchiffrement fonctionne avec un système de cryptographie asymétrique (clé privée/clé publique) pour protéger une clé de session secrète (cryptographie symétrique). La clé de session est protégée par le certificat du destinataire.

B.Correspondance_Données_Internes/Externes
Les données internes à la TOE possèdent souvent une représentation différente de celles présentées à l'utilisateur ou entrées dans la TOE.
La correspondance entre la représentation externe et la représentation interne d'une même donnée nécessite d'être protégée en 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 à l'utilisateur.

3.2 Sujets

S.Utilisateur : L'utilisateur interagit avec la TOE pour signer, chiffrer ou déchiffrer un ou plusieurs documents selon une politique de signature ou de chiffrement. L'utilisateur peut être, soit une personne physique, soit un programme appelant la TOE par l'intermédiaire du SDK.

S.Verificateur : 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.

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

- gestion de la correspondance, précisée dans la politique de signature ou de chiffrement, entre les formats de document autorisés et les applications permettant leur présentation à l'utilisateur.
- gestion du paramètre, précisée dans la politique de signature, déterminant si la TOE peut signer un document jugé instable.
- édite les fichiers de configuration de la TOE (notamment les fichiers de politique de signature et/ou de chiffrement) et les signe pour assurer leur intégrité.
- gère la correspondance, précisée dans la politique de signature, entre les formats de document présentés et les applications permettant leur présentation au vérificateur. Cette liste est précisée dans la politique de signature.
- gère la correspondance, précisée dans la politique de signature, entre les formats de document et les applications permettant de garantir la stabilité de sémantique du document dans le temps. Cette liste est précisée dans la politique de signature.

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)

3.3 Hypothèses

3.3.1 Hypothèses sur l'environnement d'utilisation

3.3.1.1 Hypothèses sur la machine hôte

H.Machine_Hôte

On suppose que la machine hôte sur laquelle la TOE s'exécute est soit directement sous la responsabilité de l'utilisateur, soit sous le contrôle de l'organisation à laquelle l'utilisateur appartient ou dont il est le client.

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 sont 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 à différencier par rapport au rôle d'administrateur de sécurité de la TOE qui a des prérogatives particulières vis-à-vis de la gestion des biens sensibles de la TOE et de ses paramètres de configuration.

3.3.1.2 Hypothèses relatives au dispositif de création de signature

H.Dispositif_De_Création_De_Signature

On suppose que le SCDev a notamment pour fonction de générer effectivement la signature à partir des éléments communiqués par la TOE. Le SCDev est également utilisé pour stocker la clé privée de déchiffrement des fichiers.

On suppose de plus qu'il est en charge de l'authentification de l'utilisateur pour lui permettre ou non d'utiliser la clé privée correspondant au certificat sélectionné pour les opérations de signature ou de déchiffrement.

Le SCDev est ainsi directement en charge de la protection des données propres de l'utilisateur.

Les données suivantes sont supposées être stockées et utilisées de manière sûre par le SCDev:

- la(les) clé(s) privée(s) de l'utilisateur, protégées en confidentialité et en intégrité,
- le(s) certificat(s) de l'utilisateur, protégés en intégrité, à défaut une référence non ambigue à ce(s) certificat(s),
- l'association clé privée/certificat, protégée en intégrité,
- Biens relatifs à l'authentification de l'utilisateur,
- les données d'authentification de l'utilisateur, protégées en intégrité et en confidentialité.
- l'association entre des données d'authentification et le couple clé privée/certificat, protégée en intégrité (1).

(1) A noter que l'association peut porter sur une donnée d'authentification et un couple clé privée/certificat. Ainsi, plusieurs couples peuvent être stockés dans le même SCDev. On peut imaginer que leur accès soit protégé par des données d'authentification différentes.

H.Communication_TOE/SCDev

On suppose que l'ensemble des composants logiciels et/ou matériels assurant l'interface entre la TOE et le SCDev est capable de gérer (ouvrir / fermer) un canal de communication garantissant l'intégrité et l'exclusivité de la communication.

H.Authentification_Utilisateur

On suppose que les composants logiciels et matériels permettant à l'utilisateur de s'authentifier auprès du SCDev pour qu'il active la clé privée de signature ou de déchiffrement correspondant au certificat sélectionné assurent la confidentialité et garantissent l'intégrité des données d'authentification au moment de la saisie et au moment du transfert de ces données vers le SCDev.

3.3.1.3 Présentation du document

H.Présentation_Du_Document

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

- soit retranscrivent fidèlement le type du document à signer ou à vérifier,
- soit préviennent le signataire ou 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.Présentation_Signatures_Existantes

Dans le cas d'une contre-signature, on suppose que le signataire dispose d'un moyen de connaître au moins l'identité du ou des signataires précédents, et au mieux vérifie cette ou ces signatures.

3.3.1.4 Hypothèse concernant l'invariance de la sémantique du document

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 (ou du document à signer) est bien invariante et de communiquer le statut de son analyse à la TOE.

3.3.2 Hypothèses sur le contexte d'utilisation

H.Présence_Du_Signataire

Pour éviter la modification de la liste des documents à signer à l'insu du signataire, ce dernier est supposé rester présent entre le moment où il manifeste son intention de signer et celui où il entre les données d'authentification pour activer la clé de signature.

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.

H.Intégrité_Services

L'environnement de la TOE est supposé fournir à l'administrateur de sécurité les moyens de contrôler l'intégrité des services et des paramètres de la TOE.

H.Politique_Signature_D'Origine_Authentique

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

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.

3.4 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.

3.5 Politique de sécurité de l'organisation (OSP)

3.5.1 Politiques relatives aux opérations de chiffrement /déchiffrement

P.Conformité_Certificat_Chiffrement

Pour éviter l'utilisation de clés potentiellement corrompues, la TOE doit contrôler que le certificat sélectionné par l'utilisateur pour chiffrer un document est bien conforme à la politique de chiffrement à appliquer.

P.Validité_Certificat_Chiffrement

Pour éviter l'utilisation de clés potentiellement corrompues, la TOE doit contrôler que le certificat sélectionné par l'utilisateur pour chiffrer un document est bien utilisé durant sa période de validité.

P.Authenticité_Certificat_Chiffrement

La TOE doit contrôler qu'un chemin de certification valide (1) existe entre le certificat de chiffrement du destinataire 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 de chiffrement du destinataire par rapport au certificat racine (point de confiance).

3.5.2 Politiques relatives à la validité de la signature créée

P.Conformité_Certificat_Signataire

Pour éviter la création de signatures invalides, la TOE doit contrôler que le certificat sélectionné par le signataire est bien conforme à la politique de signature à appliquer.

P.Validité_Certificat_Signataire

Pour éviter la création de signatures invalides, la TOE doit contrôler que le certificat sélectionné par le signataire est bien utilisé durant sa période de validité.

P.Conformité_Attributs_Signature

Pour éviter la création de signatures invalides, la TOE doit contrôler:

- que les attributs de signature sélectionnés par le signataire 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_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.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.

3.5.3 Contrôle de l'invariance de la sémantique du document

P.Sémantique_Document_Invariante

La TOE doit informer l'utilisateur si la sémantique du document n'a pu être déterminée comme étant stable.

Selon la politique de signature, la TOE adopte l'un ou l'autre des comportements suivants, si la sémantique du document n'était pas déterminée comme stable:

- Soit la politique de signature impose de stopper le processus de signature.
- Soit la politique de signature ne l'impose pas, et dans ce cas la TOE doit informer le signataire et celui-ci peut alors décider d'outrepasser l'avertissement.

3.5.4 Présentation du document et des attributs de signature au signataire

P.Possibilité_De_Présenter_Le_Document

La TOE doit permettre au signataire d'accéder à une représentation fidèle du document à signer. La TOE permettra au vérificateur de visualiser le document signé (Décret 2001-272, Art 5 alinéa c).

La TOE ne permettra pas la signature d'un document s'il ne peut pas être présenté au signataire.

P.Présentation_Attributs_De_Signature

La TOE doit permettre de présenter les attributs de signature à l'utilisateur.

La TOE doit permettre de communiquer les attributs signés au vérificateur

3.5.5 Conformité aux standards

P.Algorithme_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 [DCSSI_CRYPTO].

P.Algorithmes_De_Signature/Chiffrement

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 [DCSSI_CRYPTO].

3.5.6 Interaction avec l'utilisateur

P.Signature/Chiffrement_De_Plusieurs_Document

La TOE doit permettre d'enchaîner la signature ou le chiffrement d'un nombre fini de documents, ce nombre pouvant être éventuellement de un.

Dans le cas de la signature, le consentement à signer donné par le signataire pour ce ou ces documents portera sur les mêmes attributs de signature.

P.Arrêt_Processus_Signature

L'utilisateur doit pouvoir arrêter le processus de signature à tout moment, avant l'activation de la clé de signature.

P.Consentement_Explicite

La TOE doit obliger le signataire à réaliser une suite d'opérations non triviales pour vérifier la volonté à signer du signataire, avant de lancer le processus de signature.

3.5.7 Divers

P.Association_Certificat/Clé_privée

La TOE doit donner les informations nécessaires au SCDev ou au Keystore pour qu'il puisse activer la clé de signature/chiffrement correspondant au certificat sélectionné.

P.Export_Signature_Electronique

A l'issue du processus de signature, la TOE doit transmettre au signataire la signature électronique du document comprenant au moins:

- La signature numérique du document;
- Le condensé de l'ensemble des données à signer;
- Une référence au certificat du signataire ou le certificat du signataire lui-même;
- Une référence à la politique de signature appliquée

Note d'application

D'autres informations facilitant la vérification de la signature peuvent être ajoutées (ex: une référence à la politique de signature appliquée, le certificat du signataire in extenso, un tampon d'horodatage, etc.).

P.Export_Données_Validation

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

P.Administration

La TOE doit permettre à l'administrateur de sécurité de s'authentifier afin de gérer (ajouter/supprimer) :

- les politiques de signature et de chiffrement [B.Politiques] ;
- 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 Objectifs de sécurité

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

4.1 Objectifs de sécurité pour la TOE

4.1.1 Objectifs généraux

OT.Association_Certificat/Clé_privée

La TOE devra fournir les informations nécessaires afin que le SCDev ou le Keystore puisse activer la clé de signature correspondant au certificat sélectionné.

4.1.2 Interaction avec l'utilisateur

OT.Présentation_Conforme_Des_Attributs

La TOE doit fournir au signataire une représentation des attributs de la signature conforme aux attributs qui seront signés.

OT.Consentement_Explicite

La TOE doit fournir au signataire les moyens d'exprimer explicitement (c'est-à-dire, de manière volontaire et non ambigue) son consentement pour sélectionner un document ou plusieurs documents et déclencher le processus de signature des documents sélectionnés.

OT.Abandon_Du_Processus_De_Signature

La TOE doit fournir les moyens à l'utilisateur d'interrompre le processus de signature ou de chiffrement à tout moment, avant l'activation de la clé de signature.

OT.Ensemble_De_Documents_A_Signer/Chiffrer

Après que l'utilisateur ait donné son consentement, la TOE devra garantir que l'ensemble des documents effectivement traités correspond exactement à l'ensemble des documents sélectionnés.

Si l'utilisateur donne son consentement pour un ensemble de documents, les attributs de signature utilisés pour la signature de chacun des documents devront être identiques.

OT.Communication_Attributs_Signés

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

OT.Export_Données_Validation

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

4.1.3 Application d'une politique de signature

OT.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.

OT.Chemin_De_Certification_Vérification

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 referencé dans la politique de signature.

OT.Conformité_Du_Certificat_Source_signature

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.

OT.Validité_Du_Certificat_Source_signature

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.
- que le certificat est en cours de validité au moment du chiffrement; que le certificat n'est pas révoqué au moment du chiffrement.

OT.Conformité_Des_Attributs

La TOE doit vérifier la présence et la conformité des attributs de signature sélectionnés par le signataire en regard de la politique de signature.

OT.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).

OT.Export_Signature_Electronique

A l'issue du processus de signature, la TOE devra transmettre au signataire la signature électronique du document comprenant au moins:

- La signature numérique du document.
- Le condensé de l'ensemble des données à signer.
- Une référence au certificat du signataire ou le certificat du signataire lui-même.

- Une référence à la politique de signature appliquée.

Note d'application

D'autres informations nécessaires à la conformité avec les formats de signature CMS ou Xades peuvent être présents (ex: une référence à la politique de signature appliquée, un tampon d'horodatage, etc.).

4.1.4 Application d'une politique de chiffrement

OT.Chemin_De_Certification_Chiffrement

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

- le certificat du destinataire d'un fichier chiffré, et
- un point de confiance referencé dans la politique de chiffrement.

OT.Conformité_Du_Certificat_Destinataire_Fichierchiffré

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

OT.Validité_Du_Certificat_Destinataire_Fichierchiffré

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

- l'intégrité et l'authenticité de l'origine du certificat;
- que le certificat était en cours de validité au moment du chiffrement;
- que le certificat n'était pas révoqué au moment du chiffrement.

4.1.5 Protection des données

OT.Gestion_Politiques

La TOE ne devra permettre l'administration de l'ensemble des politiques de signatures et de chiffrement qu'aux administrateurs de la TOE.

OT.Administration

La TOE devra permettre à l'administrateur de sécurité de gérer (ajouter/supprimer) :

- les politiques de signature et/ou chiffrement [B.Politiques] ;
- la table de correspondance entre les applications de visualisation et les formats de documents en entrée de la TOE [B.Correspondance_FormatDoc_Application] via la politique de signature;
- ainsi que d'inhiber la fonction de visualisation du document signé via un paramètre géré dans la politique de signature.

OT.Authentification_Administrateur

L'administrateur de sécurité de la TOE devra s'authentifier avant de pouvoir accéder aux fonctions d'administration de la TOE.

4.1.6 Opérations cryptographiques

OT.Operations_Cryptographiques

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 [DCSSI_CRYPTO].

4.1.7 Contrôle de l'invariance de la sémantique du document

OT.Contrôle_Invariance_Document

Pour chaque document à signer ou à vérifier, la TOE devra interroger un module externe chargé d'identifier si la sémantique du document est bien stable (invariante).

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

Dans ce cas, selon la politique de signature, la TOE devra adopter l'un ou l'autre des comportements suivants:

- Soit la politique de signature impose de stopper le processus de signature et la TOE doit alors stopper le processus;
- Soit la politique de signature ne l'impose pas, et dans ce cas la TOE doit informer le signataire et celui-ci peut alors décider d'outrepasser l'avertissement.

4.1.8 Présentation du ou des documents à signer

OT.Lancement_d'Applications_De_Présentation

La TOE devra pouvoir lancer une application externe pour permettre au signataire de visualiser le document à signer ou au vérificateur de visualiser le document dont la signature est à vérifier.

Pour identifier quelle application de présentation lancer, la TOE devra gérer la correspondance entre des formats pour lesquels elle autorise la signature et des applications externes.

La TOE ne devra pas permettre la signature d'un document si elle ne peut déterminer quelle application de visualisation lancer.

4.2 Objectifs de sécurité pour l'environnement opérationnel

4.2.1 Machine hôte

OE.Machine_Hôte

La machine hôte sur laquelle la TOE s'exécute devra être soit directement sous la responsabilité de l'utilisateur soit sous le contrôle de l'organisation à laquelle l'utilisateur appartient, soit les deux.

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

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 à différencier par rapport au rôle d'administrateur de sécurité de la TOE qui a des prérogatives particulières vis-à-vis de la gestion des biens sensibles de la TOE et de ses paramètres de configuration.

4.2.2 Objectifs relatifs au SCDev et à son environnement

Les objectifs de sécurité suivant portent sur le SCDev lui-même ou sur les composants de son environnement permettant l'interaction avec le signataire ou avec la TOE.

OE.Dispositif_De_Création_De_Signature

Le SCDev électronique devra avoir au moins pour fonction de générer effectivement la signature à partir des éléments communiqués par la TOE. De plus, il sera en charge de l'authentification du signataire pour lui permettre ou non d'utiliser la clé privée correspondant au certificat selectionné.

Le SCDev sera directement en charge de la protection des données propres au signataire. Les données suivantes seront stockées et utilisées de manière sûre par le SCDev:

- Biens relatifs à la génération de la signature
- la(les) clé(s) privée(s) du signataire, protégée(s) en confidentialité et en intégrité
- le(s) certificat(s) du signataire, protégé(s) en intégrité, à défaut une référence non ambigue à ce(s) certificat(s),
- l'association clé privée/certificat, protégée en intégrité
- Biens relatifs à l'authentification du signataire
- les données d'authentification du signataire, protégées en intégrité et en confidentialité.

- l'association entre des données d'authentification et le couple clé privée/certificat, protégée en intégrité

OE.Communication_TOE/SCDev

L'ensemble des composants logiciels et/ou matériels assurant l'interface entre la TOE et le SCDev devra être capable de gérer (ouvrir / fermer) un canal de communication garantissant l'intégrité et l'exclusivité de la communication.

OE.Protection_Données_Authentification_Signataire

Les composants logiques ou physiques permettant au signataire de s'authentifier auprès du SCDev pour qu'il active la clé privée de signature correspondant au certificat sélectionné devront assurer la confidentialité et garantir l'intégrité des données d'authentification au moment de leur saisie et au long du transfert de ces données vers le SCDev.

4.2.3 Présence du signataire

OE.Présence_Du_Signataire

Le signataire devra être présent entre l'instant où il manifeste son intention de signer et celui ou il entre les données d'authentification permettant d'activer la clé de signature.

Note d'application

Si pour une quelconque raison, le signataire ne peut rester présent, il se doit de recommencer le processus à son début: sélection du ou des documents à signer, sélection des attributs, etc.

4.2.4 Présentation/sémantique invariante du ou des documents à signer

OE.Présentation_Document

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

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

Dans le cas où le document à signer contient déjà des signatures, l'environnement de la TOE permettra au signataire au moins de connaître les précédents signataires, au mieux de contrôler la validité des signatures.

4.2.5 Divers

OE.Contrôle_Sémantique_Document

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

- Soit est bien invariante ;
- Soit est stable ;

- 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.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.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.

OE.Intégrité_Services

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

4.3 Argumentaire des objectifs de sécurité

4.3.1 Politique de Sécurités Organisationnelles

P.Conformité_Certificat_Signataire

L'OSP est couverte complètement par l'objectif OT.Conformité_Du_Certificat_Source_signature qui reprend les éléments de cette OSP.

P.Validité_Certificat_Signataire

L'OSP est couverte, en cas d'opération de signature, par l'objectif OT.Validité_Du_Certificat_Source_signature qui requiert que le certificat sélectionné par le signataire soit en cours de validité.

L'OSP est couverte en cas d'opération de vérification par les objectifs :

- OT.Référence_De_Temps qui requiert que la signature soit positionnée dans le temps**.**
- OT.Validité_Du_Certificat_Source_signature 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_Signature
L'OSP est couverte par l'objectif OT.Conformité_Des_Attributs en requérant que la TOE contrôle la présence et la conformité de tous les attributs de signature requis par la politique de signature.

P.Conformité_Attributs_Signés
L'OSP est couverte par l'objectif OT.Conformité_Des_Attributs qui en reprend les termes.

P.Authenticité_Certificat_Signataire
L'OSP est couverte par l'objectif OT.Chemin_De_Certification_Verification 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
L'OSP est couverte par l'objectif OT.Conformité_Données_Validation qui requiert notamment que ces données soient signées par leur émetteur.

P.Sémantique_Document_Invariante
L'OSP est couverte en cas d'opération de signature par :

- d'une part par l'objectif de sécurité sur la TOE OT.Contrôle_Invariance_Document qui requiert que la TOE interroge un module externe chargé de contrôler l'invariance de la sémantique du document et définit les deux comportements alternatifs conformes à ceux définis dans cette politique;
- d'autre part, par l'objectif de sécurité sur l'environnement OE.Contrôle_Sémantique_Document qui requiert que l'environnement de la TOE fournisse un tel module pour un document à signer

L'OSP est couverte en cas de vérification par

- d'une part par l'objectif de sécurité sur la TOE OT.Contrôle_Invariance_Document qui requiert que la TOE interroge un module externe chargé de contrôler l'invariance de la sémantique du document et communique le résultat du contrôle au vérificateur.
- d'autre part par l'objectif de sécurité sur l'environnement OE.Contrôle_Sémantique_Document qui requiert que l'environnement de la TOE fournisse un tel module

P.Possibilité_De_Présenter_Le_Document
L'OSP est couverte en cas de signature par les objectifs OT.Lancement_d'Applications_De_Présentation et OE.Présentation_Document qui requierent: d'une part que la TOE puisse lancer une application de visualisation externe en s'appuyant sur le format du document à signer, d'autre part que la TOE empêche la signature de documents pour lesquels une application de visualisation ne peut être lancée.

L'OSP est couverte en cas de vérification par les objectifs :

- OE.Présentation_Document qui requiert que l'environnement de la TOE fournisse une application permettant au vérificateur de visualiser le document signé.
- OT.Lancement_d'Applications_De_Présentation qui requiert que la TOE puisse lancer une application de visualisation fournie par l'environnement de la TOE sur demande du vérificateur

P.Présentation_Attributs_De_Signature
L'OSP est couverte en cas d'opération de signature par l'objectif OT.Présentation_Conforme_Des_Attributs qui requiert que la TOE offre au signataire une représentation des attributs de signature conforme à ceux qui seront signés.

L'OSP est couverte en cas d'opération de vérification par l'objectif OT.Communication_Attributs_Signés qui exige que la TOE présente les attributs signés au vérificateur.

P.Algorithme_De_Hachage
L'OSP est couverte complètement par l'objectif OT.Operations_Cryptographiques qui en reprend les termes.

P.Algorithmes_De_Signature
L'OSP est couverte complètement par l'objectif OT.Operations_Cryptographiques qui en reprend les termes.

P.Signature/Chiffrement_De_Plusieurs_Document
L'OSP est couverte par l'objectif OT.Ensemble_De_Documents_A_Signer/Chiffrer qui demande que:

- la TOE garantisse que les documents signés soient ceux sélectionnés par le signataire (pas d'ajout de document, pas de suppression de document, pas de substitution de documents dans la liste)
- que des attributs de signature identiques soient utilisés lorsque le consentement du signataire porte sur un ensemble de plusieurs documents

P.Arrêt_Processus_Signature
L'OSP est couverte par l'objectif OT.Abandon_Du_Processus_De_Signature en requérant que la TOE fournisse les moyens d'interrompre le processus de signature à tout moment avant l'activation de la clé privée de signature

P.Consentement_Explicite
L'OSP est couverte par l'objectif OT.Consentement_Explicite. Cet objectif oblige le signataire à exprimer sans ambiguité sa volonté de signer. De cette manière la TOE oblige à exprimer de manière explicite son consentement à signer

P.Association_Certificat/Clé_privée
L'OSP est couverte par l'objectif OT.Association_Certificat/Clé_privée qui en reprend les éléments

P.Export_Signature_Électronique
L'OSP est couverte par l'objectif OT.Export_Signature_Electronique qui en reprend les éléments

P.Export_Données_Validation
L'OSP est couverte par l'objectif OT.Export_Données_Validation qui reprend tous les éléments de celle-ci.

P.Conformité_Certificat_Chiffrement
L'OSP est couverte complètement par l'objectif OT.Conformité_Du_Certificat_Destinataire_Fichierchiffré qui en reprend tous les éléments.

P.Validité_Certificat_Chiffrement
L'OSP est couverte complètement par l'objectif OT.Validité_Du_Certificat_Destinataire_Fichierchiffré qui reprend tous les éléments de cette OSP.
P.Authenticité_Certificat_Chiffrement

L'OSP est couverte complètement par l'objectif OT.Chemin_De_Certification_Chiffrement qui reprend tous les éléments de cette OSP.

P.Administration

L'OSP est couverte d'abord par OT.Authentification_Administrateurs qui impose que les administrateurs des politiques soient authentifiés puis OT.Gestion_Politiques et OT.Administration qui imposent la présence d'une interface d'administration des politiques de signature et/ou de chiffrement.

Enfin elle est couverte 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.

4.3.2 Hypothèses

4.3.2.1 Hypothèses sur l'environnement d'utilisation

Hypothèses sur la machine hôte

H.Machine_Hôte

Cette hypothèse est couverte complètement par l'objectif OE.Machine_Hôte qui en reprend tous les éléments.

Hypothèses relatives le dispositif de création de signature

H.Dispositif_De_Création_De_Signature

L'hypothèse est couverte complètement par l'objectif OE.Dispositif_De_Création_De_Signature qui reprend tous les éléments de cette hypothèse.

H.Communication_TOE/SCDev

Cette hypothèse est couverte entièrement par l'objectif OE.Communication_TOE/SCDev qui en reprend tous les éléments.

H.Authentification_Utilisateur

Cette hypothèse est couverte entièrement par l'objectif OE.Protection_Données_Authentification_Signataire qui en reprend tous les éléments.

Présentation du document

H.Présentation_Du_Document

Cette hypothèse est couverte en totalité par l'objectif OE.Présentation_Document qui reprend tous les éléments de celle-ci.

H.Présentation_Signatures_Existantes

Cette hypothèse est couverte complètement par l'objectif OE.Présentation_Document qui reprend tous les éléments de celle-ci.

Hypothèse concernant l'invariance de la sémantique du document

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_à_Signer qui en reprend les éléments.

4.3.2.2 Hypothèses sur le contexte d'utilisation

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

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.

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
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.

4.3.3 Tableaux de Couverture

Association politiques de sécurité organisationnelles vers objectifs de sécurité (justification au §4.3.1

Politique de Sécurité Organisationnelle (OSP)	Objectifs de Sécurité
P.Conformité_Certificat_Signataire	OT.Conformité_Du_Certificat_Source_signature
P.Validité_Certificat_Signataire	OT.Validité_Du_Certificat_Source_signature OT.Référence_De_Temps
P.Conformité_Attributs_Signature	OT.Conformité_Des_Attributs
P.Conformité_Attributs_Signés	OT.Conformité_Des_Attributs
P.Authenticité_Certificat_Signataire	OT.Chemin_De_Certification_Verification
P.Authenticité/Intégrité_Données_Validation	OT.Conformité_Données_Validation
P.Présentation_Attributs_De_Signature	OT.Communication_Attributs_Signés OT.Présentation_Conforme_Des_Attributs
P.Sémantique_Document_Invariante	OT.Contrôle_Invariance_Document OE.Contrôle_Sémantique_Document
P.Possibilité_De_Présenter_Le_Document	OT.Lancement_d'Applications_De_Présentation OE.Présentation_Document
P.Algorithme_De_Hachage	OT.Operations_Cryptographiques
P.Algorithmes_De_Signature	OT.Operations_Cryptographiques
P.Signature/Chiffrement_De_Plusieurs_Document	OT.Ensemble_De_Documents_A_Signer/Chiffrer
P.Arrêt_Processus_Signature	OT.Abandon_Du_Processus_De_Signature

P.Consentement_Explicite	OT.Consentement_Explicite
P.Association_Certificat/Clé_privée	OT.Association_Certificat/Clé_privée
P.Export_Signature_Electronique	OT.Export_Signature_Electronique
P.Export_Données_Validation	OT.Export_Données_Validation
P.Conformité_Certificat_Chiffrement	OT.Conformité_Du_Certificat_Destinataire_Fichierchiffré
P.Validité_Certificat_Chiffrement	OT.Validité_Du_Certificat_Destinataire_Fichierchiffré
P.Authenticité_Certificat_Chiffrement	OT.Chemin_De_Certification_Chiffrement
P.Administration	OT.Authentification_Administrateurs OT.Gestion_Politiques OT.Administration OE.Administrateur_De_Sécurité_Sûr

Association objectifs de sécurité vers politiques de sécurité organisationnelles :

Objectifs de Sécurité	Politique de Sécurité Organisationnelle (OSP)
OT.Conformité_Du_Certificat_Source_signature	P.Conformité_Certificat_Signataire
OT.Validité_Du_Certificat_Source_signature	P.Validité_Certificat_Signataire
OT.Référence_De_Temps	P.Validité_Certificat_Signataire
OT.Conformité_Des_Attributs	P.Conformité_Attributs_Signature P.Conformité_Attributs_Signés
OT.Chemin_De_Certification_Verification	P.Authenticité_Certificat_Signataire
OT.Conformité_Données_Validation	P.Authenticité/Intégrité_Données_Validation
OT.Communication_Attributs_Signés	P.Présentation_Attributs_De_Signature
OT.Contrôle_Invariance_Document	P.Sémantique_Document_Invariante
OT.Lancement_d'Applications_De_Présentation	P.Possibilité_De_Présenter_Le_Document
OT.Présentation_Conforme_Des_Attributs	P.Présentation_Attributs_De_Signature
OT.Operations_Cryptographiques	P.Algorithme_De_Hachage P.Algorithmes_De_Signature
OT.Ensemble_De_Documents_A_Signer/Chiffrer	P.Signature/Chiffrement_De_Plusieurs_Document
OT.Abandon_Du_Processus_De_Signature	P.Arrêt_Processus_Signature
OT.Consentement_Explicite	P.Consentement_Explicite
OT.Association_Certificat/Clé_privée	P.Association_Certificat/Clé_privée
OT.Export_Signature_Electronique	P.Export_Signature_Electronique
OT.Export_Données_Validation	P.Export_Données_Validation
OT.Conformité_Du_Certificat_Destinataire_Fichierchiffré	P.Conformité_Certificat_Chiffrement
OT.Validité_Du_Certificat_Destinataire_Fichierchiffré	P.Validité_Certificat_Chiffrement
OT.Chemin_De_Certification_Chiffrement	P.Authenticité_Certificat_Chiffrement
OT.Authentification_Administrateurs	P.Administration
OT.Gestion_Politiques	P.Administration
OT.Administration	P.Administration
OE.Administrateur_De_Sécurité_Sûr	P.Administration

OE.Présentation_Document	P.Possibilité_De_Présenter_Le_Document
OE.Machine_Hôte	
OE.Communication_TOE/SCDev	
OE.Protection_Données_Authentification_Signataire	
OE.Intégrité_Services	
OE.Présence_Du_Signataire	
OE.Fourniture_Des_Données_De_Validation	
OE.Authenticité_Origine_Politique_Signature	
OE.Dispositif_De_Création_De_Signature	
OE.Contrôle_Sémantique_Document	P.Sémantique_Document_Invariante

Association hypothèses vers objectifs de sécurité pour l'environnement opérationnel (justification 4.3.2)

Hypothèses	**Objectifs de Sécurité pour l'environnement opérationnel**
H.Machine_Hôte	OE.Machine_Hôte
H.Dispositif_De_Création_De_Signature	OE.Dispositif_De_Création_De_Signature
H.Communication_TOE/SCDev	OE.Communication_TOE/SCDev
H.Authentification_Utilisateur	OE.Protection_Données_Authentification_Signataire
H.Présentation_Du_Document	OE.Présentation_Document
H.Présentation_Signatures_Existantes	OE.Présentation_Document
H.Contrôle_Invariance_Sémantique_Document	OE.Contrôle_Sémantique_Document_à_Signer
H.Présence_Du_Signataire	OE.Présence_Du_Signataire
H.Administrateur_De_Sécurité_Sûr	OE.Administrateur_De_Sécurité_Sûr
H.Intégrité_Services	OE.Intégrité_Services
H.Accès_Données_De_Validation	OE.Fourniture_Des_Données_De_Validation
H.Politique_De_Signature_D'Origine_Authentique	OE.Authenticité_Origine_Politique_Signature

Association objectifs de sécurité pour l'environnement opérationnel vers Hypothèses

Objectifs de Sécurité pour l'environnement opérationnel	**Hypothèses**
OE.Machine_Hôte	H.Machine_Hôte
OE.Dispositif_De_Création_De_Signature	H.Dispositif_De_Création_De_Signature
OE.Communication_TOE/SCDev	H.Communication_TOE/SCDev
OE.Protection_Données_Authentification_Signataire	H.Authentification_Utilisateur
OE.Présentation_Document	H.Présentation_Du_Document H.Présentation_Signatures_Existantes
OE.Contrôle_Sémantique_Document_à_Signer	H.Contrôle_Invariance_Sémantique_Document
OE.Présence_Du_Signataire	H.Présence_Du_Signataire
OE.Administrateur_De_Sécurité_Sûr	H.Administrateur_De_Sécurité_Sûr

OE.Intégrité_Services	H.Intégrité_Services
OE.Fourniture_Des_Données_De_Validation	H.Accès_Données_De_Validation
OE.Authenticité_Origine_Politique_Signature	H.Politique_De_Signature_D'Origine_Authentique

5 Définition de composants étendus

Aucun composant étendu n’est nécessaire pour cette cible de sécurité.

6 Exigences de sécurité

6.1 Exigences fonctionnelles pour la TOE

Toutes les exigences fonctionnelles pour la TOE sont extraites de la partie 2 des Critères communs [CC].

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

Dans les exigences de sécurité fonctionnelles, les deux 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	Operation	Object / Information	Security attributes
the Signer (user)	import of the document in the TOE	a document to be signed/encrypted, or a signed document to be verified	**the Signer:** - signature policy - signer's explicit agreement to sign the document if is not stable **a document:** - document's identifier - document's stability status
the Signer (user)	import of the signer's certificate into the TOE	the signer's certificate	**the Signer:** - applied signature policy **the signer's certificate:** - key usage status - QCStatement - certificate identifier
- the Signer (user) - the SCDev	transfer to the SCDev	- the data to be signed formatted - the electronic signature	**the Signer:** - applied signature policy - signer's certificate - signer's explicit agreement to sign the present non invariant document **the data to be signed formatted:** - the data to be signed format **the electronic signature:** - signature policy identifier - commitment type - claimed role - presumed signature date and time - presumed signature location
- the Signer (user) - the SCDev	export to the Signer	the electronic signature	**the SCDev** - the status of signature generation process **the electronic signature:** - the generated electronic signature - the signed document's hash - the reference to the signer's certificate - the reference of the applied signature policy

Subject	Operation	Object / Information	Security attributes
the Verifier (user)	import of the electronic signature	the electronic signature (the signature and the related signed attributes) and the signed document	**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 (user)	import of the time reference	the time reference applied to the signature	**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 (user)	import of the certificates and the revocation data	- the certificates belonging to a certification path - the revocation data needed to validate the certification path	**the Verifier:** -applied signature policy **the certificates belonging to a certification path** - key usage - QCStatement - the electronic signature status "correct" - the period of validity of the certificate the time reference - certification policy
- the Verifier (user)	communication of the status to he verifier	- validation status "correct signature"	**validation status:** - signer's public key - document's hash - document's electronic signature
The user	Encryption/decryption	The data to be encrypted/decrypted The certificate of the receiver	**Certificate:** - key usage

6.1.1 Contrôle des documents en entrée

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 user**
- **information: a document to be signed/encrypted, or a signed document to be verified**
- **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 user**
- **information: a document to be signed/encrypted, or the signed document (document's identifier, document's stability status)**
- **operation: import of the document in the TOE.**

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 signer explicitly acknowledges to bypass the control.**

Raffinement: Stability is not applicable for the encryption/decryption.

FDP_IFF.1.3/Document acceptance: The TSF shall enforce the **no additional rules**.

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

- **controls succeed.**
- **or controls bypassed.**

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

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

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,**
- **the document shall invoque an external module in charge of controlling that the semantics of the document to be signed is invariant,**
- **the document shall inform the user when the document's semantics is not stable.**

Raffinement: not applicable for the encryption/decryption.

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

FMT_MSA.3/Document acceptance: Static attribute initialisation

FMT_MSA.3.1/Document acceptance : The TSF shall enforce the **document acceptance information flow 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 acceptance :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/Selected documents: Management of security attributes

FMT_MSA.1.1/Selected documents: The TSF shall enforce the **document acceptance information flow control policy** to restrict the ability to **select** the security attributes **documents' to be signed/encrypted identifiers** to **the user**.

FMT_SMF.1/Selection of a list of documents: Specification of management functions

FMT_SMF.1.1/Selection of a list of documents: The TSF shall be capable of performing the following management functions:

- **selecting a list of documents to be signed/verified/encrypted/decrypted.**

Raffinement: The TSF shall allow the selection of documents to be signed until the signer has given his aggreement to sign.

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

FMT_MSA.1.1/Document's semantics invariance status: The TSF shall enforce the **document acceptance information flow 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.**

FMT_MSA.1/Signer agreement to sign an instable document: Management of security attributes

FMT_MSA.1.1/Signer agreement to sign an instable document: The TSF shall enforce the **document acceptance information flow control policy** to restrict the ability to **modify** the security attributes **signer agreement to sign an instable document** to the **signer**.

FMT_SMF.1/Getting signer agreement to sign an instable document: Specification of management functions

FMT_SMF.1.1/Getting signer agreement to sign an instable document: The TSF shall be capable of performing the following management functions:

- **get the explicit agreement of the signer to sign a document whose semantics is instable.**

6.1.2 Sélection du certificat de l'utilisateur

FDP_IFC.1/User's certificate import: Subset information flow control

FDP_IFC.1.1/User's certificate import: The TSF shall enforce the **User's certificate import policy** on

- **subjects: the user**
- **information: the user's certificate**
- **operations: import of the user's certificate into the TOE**

FDP_IFF.1/ User's certificate import: Simple security attributes

FDP_IFF.1.1/User's certificate import: The TSF shall enforce the **User's certificate import policy** based on the following types of subject and information security attributes:

- **subjects: the user**
- **information: the user's certificate attributes (Key usage, QC statement -for the signature operations-).**

FDP_IFF.1.2/User's certificate import: 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 signer's certificate into the TOE

- **the "key usage" of the selected 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).**

FDP_IFF.1.3/Users' certificate import: The TSF shall enforce the **rules as defined in the policy**.

FDP_IFF.1.4/Signer's certificate import The TSF shall explicitly authorise an information flow based on the following rules:

- **controls succeed.**

FDP_IFF.1.5/ Users' certificate import The TSF shall explicitly deny an information flow based on the following rules: **rules as defined in the policy.**

- **Controls fail.**

FMT_MSA.3/ User's certificate import: Static attribute initialisation

FMT_MSA.3.1/User's certificate import: The TSF shall enforce the **User's certificate import policy** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/User's certificate import [*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/User's certificate: Management of security attributes

FMT_MSA.1.1/Signer's certificate: The TSF shall enforce the **User's certificate import policy** to restrict the ability to **select** the security attributes **user's certificate** to the **user**.

FDP_ITC.2/User's certificate: Import of user data with security attributes

FDP_ITC.2.1/User's certificate: The TSF shall enforce the **User's certificate import policy** when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2/User's certificate: The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3/User's certificate: The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4/User's certificate: The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5/User's certificate: The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **no additional importation control rules.**

FPT_TDC.1/User's certificate: Inter-TSF basic TSF data consistency

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

FPT_TDC.1.2/User certificate: The TSF shall use **interpretation rules as defined in the policy** when interpreting the TSF data from another trusted IT product.

FMT_SMF.1/User's certificate selection: Specification of management functions

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

- **allow the signer to select a certificate among the list of certificates suitable for the applied signature/encryption policy.**

6.1.3 Sélection de la politique à appliquer

FMT_MTD.1/Selection of the applied 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 policy** to the **user**.

FMT_SMF.1/Selection of the applied 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 user shall be permitted to select the policy to be applied.**

FMT_MSA.1/Attributes: Management of security attributes

FMT_MSA.1.1/Attributes: The TSF shall enforce the **signature generation and encryption information flow control policy** to restrict the ability to **select** the security attributes **signature and encryption attributes** to the **user**.

FMT_SMF.1/Modification of attributes: Specification of management functions

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

- **permit the user to change the value of the attributes required by the applied signature/encryption policy.**

Raffinement: for the signature, the TSF shall allow the modification of signature attributes until the signer has given his agreement to sign.

6.1.4 Exigences relatives à la signature

6.1.4.1 Interaction avec le signataire

FDP_ITC.1/Explicit signer agreement: Import of user data without security attributes

FDP_ITC.1.1/Explicit signer agreement: The TSF shall enforce the **signature generation information flow control policy** when importing user data, controlled under the SFP, from outside of the TOE.

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

FDP_ITC.1.3/Explicit signer agreement: The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **rules for the agreement depends on the context (SDK, single signature, multisignature).**

FDP_ROL.2/Abort of the signature process: Advanced rollback

FDP_ROL.2.1/Abort of the signature process: The TSF shall enforce the **signature generation information flow control policy** to permit the rollback of all the operations on the **electronic signature and its related attributes**.

FDP_ROL.2.2/Abort of the signature process: The TSF shall permit operations to be rolled back **before the data to be signed formatted are transfered to the SCDev**.

6.1.4.2 Opérations cryptographiques

FCS_COP.1/Hash : Cryptographic operation

FCS_COP.1.1/hash: The TSF shall perform **hash generation** in accordance with a specified cryptographic algorithm **SHA 1, SHA 256, SHA 384, SHA 512** and cryptographic key sizes **160, 256, 384, 512** that meet the following: [**DCSSI_CRYPTO**].

6.1.4.3 Transfert de données à signer au SCDev

FDP_IFC.1/Signature generation: Subset information flow control

FDP_IFC.1.1/Signature generation: The TSF shall enforce the **signature generation information flow control policy** on

- **subjects: the signer, the SCDev**
- **information:**
  - **the data to be signed formatted**
  - **the numeric signature (once generated)**
    - **operations:**
  - **transfert to the SCDev**

FDP_IFF.1/Signature generation: Simple security attributes

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

- **subjects: the signer (applied signature policy, signer's certificate), signer's explicit agreement to sign the present non invariant document, the SCDev**
- **information: the data to be signed formatted (the data to be signed format), the electronic signature (signature policy identifier, commitment type, claimed role, presumed signature date and time, presumed signature location.**

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

Transfer of the data to be signed formatted:

- **communicate the signature attributes to the signer before the signature generation**
- **launch the viewer corresponding to the document's format according to the document format/viewer association table**
- **activate the signing key corresponding to the selected signer's certificate.**

Electronic signature:

- **if the signature policy requires the inclusion of the signature attribute "signature policy identifier", then its value shall be included;**
- **if the signature policy requires the inclusion of the signature attribute "commitment type", then its value shall be included;**
- **if the signature policy restricts the values to be taken by the "commitment type" attribute, then its value shall be conformant to the signature policy;**
- **if the signature policy requires the inclusion of the signature attribute "claimed role", then its value shall be included;**
- **if the signature policy restricts the values to be taken by the "claimed role" attribute then its value shall be conformant to the signature policy;**

- **if the signature policy prevents the inclusion of the signature attribute "presumed signature date and time", then its value shall not be included;**
- **if the signature policy requires the inclusion of the signature attribute "presumed signature location", then its value shall be included;**
- **and additional rules as defined in the policy**

FDP_IFF.1.3/Signature generation The TSF shall enforce the **rules as defined in the policy**.

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

- **Security attributes are compliant to Signature SFP**
- **and the data to be signed formatted semantic control succeed.**

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

- **Security attributes are not compliant to the Signature SFP**
- **or the data to be signed formatted semantic control fails.**

FMT_MSA.3/Signature generation: Static attribute initialisation

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

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

6.1.4.4 Récupération de la signature électronique

FDP_IFC.1/Electronic signature export Subset information flow control

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

- **subjects:**
  - **the signer,**
  - **the SCDev**
- **information:**
  - **the generated numeric signature**
  - **the signature attributes: document's hash, reference to the signer's certificate**
- **operations:**
  - **export to the signer.**

FDP_IFF.1/Electronic signature export: Simple security attributes

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

- **subjects:**
  - **the signer (signer's security attributes)**
  - **the SCDev (the status of signature generation process, any other SCDev attributes)**
- **information:**
  - **the electronic signature (the generated numeric signature, the signed document's hash, the reference to the signer's certificate, the reference of the applied signature policy, list of signature attributes**

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

Export of the electronic signature to the signer is allowed if the signature generation (performed by the SCDev) succeeded.

FDP_IFF.1.3/Electronic signature export: The TSF shall enforce the **other rules explicitly defined in the signature policy.**

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

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

FDP_ETC.2/Electronic signature export: Export of user data with security attributes

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

FDP_ETC.2.2/Electronic signature export: The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3/Electronic signature export: 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/Electronic signature export: The TSF shall enforce the following rules when user data is exported from the TOE: **no additional exportation control rules**

FMT_MSA.3/Electronic signature export: Static attribute initialisation

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

FMT_MSA.3.2/Electronic signature export: 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/SCDev signature generation status: Management of security attributes

FMT_MSA.1.1/SCDev signature generation status: The TSF shall enforce the **electronic signature export information flow control policy** to restrict the ability to **modify** the security attributes **SCDev's signature generation status** to **nobody**.

FMT_SMF.1/Getting SCDev's signature generation status: Specification of management functions

FMT_SMF.1.1/Getting SCDev's signature generation status: The TSF shall be capable of performing the following management functions:

- **getting the SCDev's signature generation status (discriminate whether the signature generation process completed or failed)..**

6.1.5 Exigences relatives à la vérification de signature

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

6.1.5.1 Récupération de la signature à vérifier et des 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 signature and related signed attributes, and the signed document**
- **operation: import (i.e. acceptance as signed attributes conforming to the 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, other verifier's attributes, if any)**
- **information: electronic signature (the signed attributes, list of supported signed attributes) and the signed document (the signed document's content format, 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**
- **and other supported rules as defined in the policy**

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.**

FMT_MSA.3/Electronic signature: Static attribute initialisation

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

FMT_MSA.3.2/Electronic signature: 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 information flow 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:

- **invoke 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.**

6.1.5.2 Opérations cryptographiques

FCS_COP.1/Signature verification: Cryptographic operation

FCS_COP.1.1/Signature verification: The TSF shall perform **digital signature verification** in accordance with a specified cryptographic algorithm **RSA** and cryptographic key sizes **1024, 2048** that meet the following: [**DCSSI_CRYPTO**].

6.1.5.3 Export des résultats de la 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 (verifier's security attributes)**
- **information: validation status "correct signature" (signer's public key, document's hash, document's numeric 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 numeric 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 **verification policy.**

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.**

6.1.5.4 Import d'une référence de temps fiable

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, other verifier's attributes, if any)**
- **information: the time reference applied to the signer's numeric 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 no **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 information flow control policy** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/Time reference: 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 information flow control polic**y 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: **importation rules as defined in the policy**.

6.1.6 Vérification du chemin de certification

Les exigences qui suivent se rapportent à la vérification du chemin de certification nécessaire pour les opérations de vérification de signature et de chiffrement.

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 acceptanced 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)

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.**

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).**

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)**

FDP_IFF.1.3/Certification path: The TSF shall enforce the **rules as defined in the validation policy**.

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 fails**.

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: 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.**

6.1.7 Conformité aux standards

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 **CMS, XML/DSIG, XADES-T standard** when interpreting the TSF data from another trusted IT product.

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

FPT_TDC.1.1/Encryption: The TSF shall provide the capability to consistently interpret **encrypted files** when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/Encryption: The TSF shall use **CMS, XML_Enc standard** when interpreting the TSF data from another trusted IT product.

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 **RFC-3161** when interpreting the TSF data from another trusted IT product.

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 **X509 v3 standard** when interpreting the TSF data from another trusted IT product.

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 **CRL V2 standard** when interpreting the TSF data from another trusted IT product.

6.1.8 Exigences relatives au chiffrement

6.1.8.1 Opérations cryptographiques

FCS_COP.1/Encryption : Cryptographic operation

FCS_COP.1.1/Encryption: The TSF shall perform **encryption** in accordance with a specified cryptographic algorithm **AES** and cryptographic key sizes **128, 192, 256** that meet the following: [**DCSSI_CRYPTO**].

FCS_CKM.1/Encryption session keys: Cryptographic key generation

FCS_CKM.1.1/Encryption: The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **AES** and specified cryptographic key sizes **128, 192, 256** that meet the following: [**DCSSI_CRYPTO**].

Raffinement : generation of session keys

FCS_CKM.4/Encryption session keys: Cryptographic key destruction

FCS_CKM.4.1/Encryption: The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **Zeroization of all plaintext cryptographic keys**.

Raffinement : destruction of generated session keys

6.1.9 Exigences relatives au déchiffrement

6.1.9.1 Opérations cryptographiques

FCS_COP.1/Decryption : Cryptographic operation

FCS_COP.1.1/decryption The TSF shall perform **decryption** in accordance with a specified cryptographic algorithm **AES** and cryptographic key sizes **128, 192, 256** that meet the following: [**DCSSI_CRYPTO**].

6.1.10 Identification et authentification des utilisateurs

FIA_UID.2 User identification: before any action

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

FIA_UAU.1/Administrator authentication: Timing of authentication

FIA_UAU.1.1/Administrator authentication: The TSF shall allow any actions on behalf of the user to be performed before the user is authenticated, except the following administration operations:

- **Management of the viewer activation parameter.**
- **Management of the document format/viewer association table.**
- **Management of the signature policies set.**

FIA_UAU.1.2/Administrator authentication: The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.11 Administration de la TOE

6.1.11.1 Gestion des politiques

FMT_MTD.1/Management of the policies: Management of TSF data

FMT_MTD.1.1/Management of the policies: The TSF shall restrict the ability to **add and remove** the signature policies to **the security administrator of the TOE**.

FMT_SMF.1/Management of the policies: Specification of management functions

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

- **permit an administrator of the TOE to add and remove signature/encryption policies to / from the set of policies the TOE supports.**

6.1.11.2 Gestion des roles

FMT_SMR.1: Security roles

FMT_SMR.1.1: The TSF shall maintain the roles.

- **user**
- **security administrator.**

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

6.1.11.3 Capacité à présenter le document au signataire

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 association table: Specification of management functions

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

- **allow the administrator of the TOE to manage operations as definied in the policy 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: 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.**

6.2 Exigences d'assurance pour la TOE

Le niveau visé est **EAL3 augmenté** du composant ALC_FLR.3.

Exigences		Intitulés
Classe ADV : Development		
	ADV_ARC.1	Security architecture description
	ADV_FSP.3	Functional specification with complete summary
	ADV_TDS.2	Architectural design
Classe AGD : Guidance documents		
	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Classe ALC : Life-cycle support		
	ALC_CMC.3	Autorisation controls
	ALC_CMS.3	Implementation representation CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_FLR.3	Systematic flaw remediation
	ALC_LCD.1	Developer defined life-cycle model
Classe ASE : Security Target Evaluation		
	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Classe ATE : Tests		
	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing : basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Classe AVA : Vulnerability assessment		
	AVA_VAN.2	Vulnerability analysis

Toutes les exigences d'assurance pour la TOE sont extraites de la partie 3 des Critères communs [CC].

6.3 Argumentaire des exigences de sécurité

6.3.1 Couverture des objectifs de sécurité

L'argumentaire des profils de protection est augmenté des argumentaires de couverture des objectifs de sécurité suivants :

OT.Association_Certificat/Clé_privée
L'objectif est couvert par l'exigence FDP_IFF.1/Signature generation. Cette exigence requiert que la TOE soit capable d'activer la clé privée de signature correspondant au certificat sélectionné par le signataire.

OT.Présentation_Conforme_Des_Attributs
L'objectif est couvert par l'exigence fonctionnelle FDP_IFF.1/Signature generation qui requiert notamment que la TOE puisse présenter les attributs de signature au signataire avant le début du processus de signature.

OT.Consentement_Explicite
L'objectif est couvert par l'exigence FDP_ITC.1/Explicit signer agreement par laquelle la TOE impose qu'une suite d'opérations non triviales soit réalisée avant de considérer la volonté de signer comme effective.

OT.Abandon_Du_Processus_De_Signature
L'objectif est couvert par le composant d'exigence FDP_ROL.2/Abort of the signature process qui assure que le signataire a la possibilité d'annuler la signature avant l'envoi des données au SCDev.

OT.Ensemble_De_Documents_A_Signer/Chiffrer
L'objectif est couvert par les exigences fonctionnelles:

- *FMT_MSA.1/Selected documents qui restreint la capacité à sélectionner des documents à signer/chiffrer au seul utilisateur.*
- *FMT_SMF.1/Selection of a list of documents qui requiert que la TOE offre la possibilité de sélectionner des documents à signer/chiffrer tant que l'utilisateur n'a pas donné sont agrément à signer.*
- *FMT_MSA.1/Attributes qui restreint au seul utilisateur la capacité de sélectionner les attributs.*
- *FMT_SMF.1/Modification of attributes qui requiert que la TOE offre la possibilité de modifier la valeur des attributs tant que l'utilisateur n'a pas donné sont agrément à signer.*

De facto, les mêmes attributs de signature seront appliqués à tous les documents sélectionnés.

OT.Communication_Attributs_Signés
L'objectif de sécurité 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.

OT.Export_Données_Validation
L'objectif de sécurité 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.

OT.Référence_De_Temps

L'objectif de sécurité 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 policy et FMT_SMF.1/Selection of the applied 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.*

OT.Chemin_De_Certification_Vérification

L'objectif de sécurité 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 policy et FMT_SMF.1/Selection of the applied 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.*

OT.Conformité_Du_Certificat_Source_signature

L'objectif de sécurité est couvert de la manière suivante:
La TOE doit appliquer une politique de contrôle de flux d'informations lors de l'import d'un certificat (FDP_IFC.1/User's certificate import). Le composant fonctionnel FDP_IFF.1/User's certificate import définit que cette politique de contrôle de flux permettra effectivement l'import du certificat dans la TOE si des règles définies dans la politique de signature sont bien remplies. Ces règles portent sur le certificat du signataire. La conformité du certificat sélectionné est garantie si les attributs de celui-ci remplissent le sous-ensemble de règles défini dans la politique de signature.
Les composants fonctionnels FDP_ITC.2/User's certificate et FPT_TDC.1/User's certificate assurent d'une part que la TOE applique les règles de la politique de contrôle de flux lors de l'import du certificat sélectionné et d'autre part que la TOE est en mesure d'exploiter les données contenues dans le certificat importé.
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/User's certificate import 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/User's certificate et FMT_SMF.1/Uer's certificate selection garantissent au signataire le droit exclusif de sélectionner le certificat approprié pour une signature électronique qu'il souhaite réaliser.*
- *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.*

OT.Validité_Du_Certificat_Source_signature

L'objectif de sécurité est couvert de la manière suivante:
La TOE doit appliquer une politique de contrôle de flux d'informations lors de l'import d'un certificat (FDP_IFC.1/User's certificate import). Le composant fonctionnel FDP_IFF.1/User's certificate import définit que cette politique de contrôle de flux permettra effectivement l'import du certificat dans la TOE si des règles définies dans la politique de signature sont bien remplies. Ces règles portent sur le certificat du signataire. La conformité du certificat sélectionné est garantie si les attributs de celui-ci remplissent le sous-ensemble de règles défini dans la politique de signature.
Les composants fonctionnels FDP_ITC.2/User's certificate et FPT_TDC.1/User's certificate assurent d'une part que la TOE applique les règles de la politique de contrôle de flux lors de l'import du certificat sélectionné et d'autre part que la TOE est en mesure d'exploiter les données contenues dans le certificat importé.
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/User's certificate import 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/User's certificate et FMT_SMF.1/User's certificate selection garantissent au signataire le droit exclusif de sélectionner le certificat approprié pour une signature électronique qu'il souhaite réaliser.*
- *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.*

OT.Conformité_Des_Attributs

L'objectif de sécurité est couvert de la manière suivante:
La TOE doit appliquer une politique de contrôle de flux d'informations lors de la génération d'une signature (FDP_IFC.1/Signature generation). Le composant fonctionnel FDP_IFF.1/Signature generation définit que cette politique de contrôle de flux permettra la génération de la signature (c'est-à-dire l'envoi des données à signer formatées au SCDev) si des règles définies dans la politique de signature sont bien remplies. Ce dernier composant comprend également des règles relatives aux attributs de la signature. La conformité des attributs de signature est garantie si ces attributs remplissent le sous-ensemble de règles défini dans la politique de signature.
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 generation 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/Attributes et FMT_SMF.1/Modification of attributes garantit au signataire le droit exclusif de sélectionner le certificat approprié pour une signature électronique qu'il souhaite réaliser.*
- *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.*

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 policy et FMT_SMF.1/Selection of the applied 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:

o 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.

o 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:

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

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

OT.Conformité_Données_Validation

L'objectif de sécurité 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 policy et FMT_SMF.1/Selection of the applied 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.*

OT.Export_Signature_Electronique

L'objectif de sécurité 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/Electronic signature export). Le composant fonctionnel FDP_IFF.1/Electronic signature export définit les règles à appliquer par la TOE pour accepter de retourner la signature électronique.
Le composant FDP_ETC.2/Electronic signature export 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/Electronic signature export 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_SMF.1/Getting SCDev's signature generation status requiert que la TOE soit capable de recevoir du SCDev le statut de l'opération de génération de la signature numérique.*
- *Le composant fonctionnel FMT_MSA.1/SCDev signature generation status qui ne permet à personne de modifier le statut de l'opération de génération de la signature retourné par le SCDev.*
- *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.*

OT.Operations_Cryptographiques

Outre la couverture de cet objectif par les exigences issues des profils de protection, l'objectif est aussi couvert par FCS_COP.1/Encryption, FCS_CKM.1/Encryption session keys, FCS_CKM.4/Encryption session keys et FCS_COP.1/Decryption. Le format des fichiers à chiffrer est défini par FPT_TDC.1/Encryption.

OT.Chemin_De_Certification_Chiffrement

L'objectif de sécurité OT.Chemin_De_Certification est couvert de la manière suivante:
La TOE doit appliquer une politique de contrôle de flux d'informations (FDP_IFC.1FDP_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. 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 policy et FMT_SMF.1/Selection of the applied 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 operation avant d'avoir identifié l'utilisateur.*

OT.Conformité_Du_Certificat_Destinataire_Fichierchiffré

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. 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 policy et FMT_SMF.1/Selection of the applied 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 operation avant d'avoir identifié l'utilisateur.*

OT.Validité_Du_Certificat_Destinataire_Fichierchiffré

L'objectif de sécurité O.Validié_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. Ces exigences 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 policy et FMT_SMF.1/Selection of the applied 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 operation avant d'avoir identifié l'utilisateur.*

OT.Administration

L'objectif est couvert par les composants fonctionnels suivants:

- *FMT_SMR.1 qui requiert que la TOE différencie le rôle d'administrateur de sécurité du rôle de signataire;*
- *FMT_MTD.1/Document format/viewer association table et FMT_SMF.1/Management of the document format/viewer association table qui permettent à l'administrateur de sécurité de la TOE (et uniquement lui) de modifier la table d'association entre les formats de documents et les programmes de visualisation;*
- *FMT_SMF.1/Management of the viewer activation parameter qui définit la function permettant d'inhiber la fonction de visualisation du document signé*
- *FMT_SMF.1/Management of the signature policies qui définissent les opérations de gestion applicables aux politiques de signature et FMT_MTD.1/Management of the signature policies qui restreint leur utilisation au seul administrateur de sécurité de la TOE.*

OT.Authentification_Administrateur

L'objectif est directement couvert par l'exigence FIA_UAU.1/Administrator authentication qui exige l'authentification de l'administrateur pour pouvoir accéder aux fonctions de configuration de la politique.

OT.Gestion_Politiques

L'objectif est directement couvert par les exigences FMT_MTD.1/Management of the policies et FMT_SMF.1/Management of the policies qui imposent que l'administrateur de sécurité puisse gérer (ajout/suppression) les politiques.

OT.Contrôle_Invariance_Document

L'objectif de sécurité 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.*
- *Les composants fonctionnels FMT_MSA.1/Signer agreement to sign an instable document et FMT_SMF.1/Getting signer agreement to sign an instable document garantissent que seul le signataire peut modifier l'attribut permettant à la TOE de continuer le processus de signature d'un document dont la sémantique n'est pas déterminée comme stable.*
- *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.*

OT.Lancement_d'Applications_De_Présentation

L'objectif de sécurité est couvert par les composants d'exigence suivants:

- *FDP_IFF.1/Signature generation, 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 garantit 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*.

6.3.2 Satisfaction des dépendances

Exigences	Dépendances CC	Dépendances Satisfaites
FDP_IFC.1/Signature generation	(FDP_IFF.1)	FDP_IFF.1/Signature generation
FDP_IFF.1/Signature generation	(FDP_IFC.1) et (FMT_MSA.3)	FDP_IFC.1/Signature generation, FMT_MSA.3/Signature generation
FMT_MSA.3/Signature generation	(FMT_MSA.1) et (FMT_SMR.1)	FMT_SMR.1, FMT_MSA.1/Attributes, FMT_MSA.1/Signer's certificate
FDP_ITC.1/Explicit signer agreement	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_MSA.3)	FDP_IFC.1/Signature generation, FMT_MSA.3/Signature generation
FDP_IFC.1/Electronic signature export	(FDP_IFF.1)	FDP_IFF.1/Electronic signature export
FDP_IFF.1/Electronic signature export	(FDP_IFC.1) et (FMT_MSA.3)	FDP_IFC.1/Electronic signature export, FMT_MSA.3/Electronic signature export
FDP_ETC.2/Electronic signature export	(FDP_ACC.1 ou FDP_IFC.1)	FDP_IFC.1/Electronic signature export
FMT_MSA.3/Electronic signature export	(FMT_MSA.1) et (FMT_SMR.1)	FMT_MSA.1/SCDev signature generation status, FMT_SMR.1
FMT_MSA.1/SCDev signature generation status	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FDP_IFC.1/Electronic signature export, FMT_SMF.1/Getting SCDev's signature generation status, FMT_SMR.1
FMT_SMF.1/Getting SCDev's signature generation status	Pas de dépendance	
FMT_MSA.1/Selected documents	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FMT_SMR.1, FDP_IFC.1/Document acceptance, FMT_SMF.1/Selection of a list of documents
FMT_SMF.1/Selection of a list of documents	Pas de dépendance	
FMT_MSA.1/Signer agreement to sign an instable document	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FMT_SMR.1, FDP_IFC.1/Document acceptance, FMT_SMF.1/Getting signer agreement to sign an instable document
FMT_SMF.1/Getting signer agreement to sign an instable document	Pas de dépendance	
FMT_MSA.1/Attributes	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FDP_IFC.1/Signature generation, FMT_SMR.1, FMT_SMF.1/Modification of signature attributes
FMT_SMF.1/Modification of signature attributes	Pas de dépendance	
FDP_IFC.1/Signer's certificate import	(FDP_IFF.1)	FDP_IFF.1/Signer's certificate import
FDP_IFF.1/Signer's certificate import	(FDP_IFC.1) et (FMT_MSA.3)	FDP_IFC.1/Signer's certificate import, FMT_MSA.3/User's certificate import

Exigences	Dépendances CC	Dépendances Satisfaites
FMT_MSA.3/User's certificate import	(FMT_MSA.1) et (FMT_SMR.1)	FMT_SMR.1, FMT_MSA.1/Signer's certificate
FMT_MSA.1/Signer's certificate	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FMT_SMR.1, FDP_IFC.1/Signer's certificate import, FMT_SMF.1/Signer's certificate selection
FDP_ITC.2/Signer's certificate	(FDP_ACC.1 ou FDP_IFC.1) et (FPT_TDC.1) et (FTP_ITC.1 ou FTP_TRP.1)	FDP_IFC.1/Signer's certificate import, FPT_TDC.1/Signer's certificate
FPT_TDC.1/Signer's certificate	Pas de dépendance	
FMT_SMF.1/Signer's certificate selection	Pas de dépendance	
FMT_MTD.1/Management of the signature policies	(FMT_SMF.1) et (FMT_SMR.1)	FMT_SMR.1, FMT_SMF.1/Management of the signature policies
FMT_SMF.1/Management of the signature policies	Pas de dépendance	
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
FDP_ROL.2/Abort of the signature process	(FDP_ACC.1 ou FDP_IFC.1)	FDP_IFC.1/Signature generation
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

Exigences	Dépendances CC	Dépendances Satisfaites
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 policy	(FMT_SMF.1) et (FMT_SMR.1)	FMT_SMR.1, FMT_SMF.1/Selection of the applied policy
FMT_SMF.1/Selection of the applied 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

Exigences	Dépendances CC	Dépendances Satisfaites
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
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
FPT_TDC.1/Encryption	Pas de dépendance	
FCS_COP.1/Encryption	(FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2) et (FCS_CKM.4)	FCS_CKM.1/Encryption session keys et FCS_CKM.4/Encryption session keys
FCS_CKM.1/Encryption session keys	(FCS_CKM.2 ou FCS_COP.1) et FCS_CKM.4	FCS_COP.1/Encryption et FCS_CKM.4/Encryption session keys

Exigences	Dépendances CC	Dépendances Satisfaites
FCS_CKM.4/Encryption session keys	(FDP_ITC.1 ou FDP_ITC.2 ou FCS_CKM.1)	FCS_CKM.1/Encryption session keys
FCS_COP.1/Decryption	(FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2) et (FCS_CKM.4)	FDP_ITC.2/Signer's certificate et FCS_CKM.4/Encryption session keys
FIA_UAU.1/Administrator authentication	(FIA_UID.1)	FIA_UID.2

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 function 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:

- o 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).
- o 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.
- o 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.

La dépendance FTP_ITC.1 or FTP_TRP.1 de FDP_ITC.2/Signer's certificate n'est pas supportée. La dépendance entre le composant d'exigence *FDP_ITC.2/Signer's certificate* et un des composants *FTP_ITC.1* ou *TFP_TRP.1* n'est pas satisfaite car les protocoles utilisés dans les infrastructures à clé publiques sont autoprotégés et garantis, non pas immédiatement, mais au moment de la vérification de la signature:

- o l'intégrité des certificats de la chaine de certification est garantie grâce au certificat autosigné (ou point de confiance) défini dans la politique de signature, qui est elle-même maintenue intègre par l'environnement de la TOE
- o lors de la vérification de la signature, le fait de construire une chaine de certification valide entre le certificat du signataire et le 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 chaine.
- o enfin, le certificat du signataire, ne nécessite pas de protection en termes de confidentialité.

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

7 Spécifications globales de la TOE

7.1 Fonctions de sécurité de la TOE

7.1.1 Fonctions d'authentification

F.Authentification_Utilisateur

Cette fonction permet de réaliser l'authentification de l'utilisateur avant toute action de signature ou de déchiffrement.

Elle s'appuie sur la ressource support des données d'authentification configurée par la fonction d'administration.

Elle récupère les données de configuration de l'utilisateur, les paramètres de configuration du support d'identification. Elle vérifie l'accès à ce support suite à la fourniture d'un code PIN par l'utilisateur.

Exigences	Argumentaire de couverture
Authentification des utilisateurs	
FIA_UID.2	L'utilisateur doit être identifié
FIA_UAU.1/Administrator authentication	Seules les operations de selection des visualiseur de documents et de sélection de certains parameters autorisés par la politique appliqués sont accessibles sans authentification

7.1.2 Fonctions de signature

F.Signature

Cette fonction permet de réaliser une signature (ou une sur-signature ou une co-signature) suivant les standards suivants :

- CMS (pour les opérations de signature, sur-signature et co-signature);
- XMLDSIG;
- XADES_T.

Elle prend en entrée les paramètres suivants :

- Un document à signer (voire un document possédant une ou plusieurs signatures attachées dans le cas de la sur-signature ou de la co-signature).
- La politique de signature à appliquer.

Ces paramètres sont sélectionnés via l'interface applicative de la TOE ou via les informations fournies au SDK par une application appelante.

Elle récupère un profil de signature à appliquer issu de la politique de signature.

Elle exploite les paramètres de ce profil afin d'effectuer :

- les opérations de contrôle de stabilité sémantique,
- la présentation du document.
- l'utilisation et la présentation des attributs à signer (référence politique, engagement…) (sauf XMLDSIG).

- la validation du certificat de signature.
- la génération d'une requête pour horodater la signature (CMS uniquement).

Dans le cas de la sur-signature ou de la co-signature, la fonction vérifie également les signatures déjà apposées sur le document.

Elle demande à l'utilisateur de sélectionner le certificat de signature parmi ceux présents sur le SCDEV puis de s'authentifier pour accéder aux informations du SCDEV par appel à la fonction Authentification.

Elle formate les données à signer au format sélectionné par l'utilisateur puis calcule le condensé de ces données selon l'algorithme de hashage précisé par la politique et ensuite transfère le condensé au SCDev afin que ce dernier effectue une signature au format PKCS#1 en utilisant la référence de la clé privée de l'utilisateur (correspondant au certificat de signature sélectionné).

La fonction récupère la signature numérique générée par le SCDev

Le document signé ainsi généré est alors fourni à l'utilisateur ou à l'application appelante via le SDK.

Remarque: en cas d'instabilité détectée, la fonction de signature demande à l'utilisateur s'il souhaite poursuivre l'opération ce qui de ce fait implique qu'il n'est pas possible de forcer la signature de documents non stables sans volonté du signataire.

Exigences	Argumentaire de couverture
Sélection de la politique à appliquer	
FMT_MTD.1/Selection of the applied policy	L'utilisateur peut sélectionner la politique qu'il souhaite utiliser pour signer ou chiffrer.
FMT_SMF.1/ Selection of the applied policy	L'utilisateur peut sélectionner la politique qu'il souhaite utiliser pour signer ou chiffrer.
FMT_MSA.1/Attributes	L'utilisateur peut sélectionner certains attributs de la politique qu'il souhaite utiliser pour signer ou chiffrer.
FMT_MSA.3/Signature generation	L'utilisateur peut sélectionner certains attributs de la politique qu'il souhaite utiliser pour signer ou chiffrer.
FMT_SMF.1/Modification of attributes	L'utilisateur peut sélectionner certains attributs de la politique qu'il souhaite utiliser pour signer ou chiffrer.
Selection du certificat de l'utilisateur	
FDP_IFC.1/User's certificate import	L'utilisateur peut selectionner son certificat à utiliser
FDP_IFF.1/ User's certificate import	
FMT_MSA.3/ User's certificate import	L'utilisateur peut selectionner son certificat à utiliser
FMT_MSA.1/ User's certificate	L'utilisateur peut selectionner son certificat à utiliser
FDP.ITC.2/ User's certificate	L'utilisateur peut selectionner son certificat à utiliser
FPT_TDC.1/ User's Certificate	L'utilisateur peut selectionner son certificat à utiliser
FMT_SMF.1/ User's certificat selection	L'utilisateur peut selectionner son certificat à utiliser
Contrôle des documents en entrée	
FDP_IFC.1/Document acceptance	La stabilité du document est contrôlée avant sa signature
FDP_IFF.1/Document acceptance	
FDP_ITC.1/Document acceptance	Seuls les documents dont la sémantique est invariable sont acceptés
FMT_MSA.3/Document acceptance	Il est impossible de forcer la signature de documents non stables
FMT_MSA.1/Selected Document	L'utilisateur peut sélectionner les documents à signer/verifier/chiffrer/déchiffrer
FMT_SMF.1/Selection of list of documents	L'utilisateur peut sélectionner les documents à signer/verifier/chiffrer/déchiffrer
FMT_MSA.1/Document's semantics invariance status	Il est impossible de forcer la signature de documents non stables
FMT_SMF.1/Getting document's semantics invariance status	La TOE peut appeler une application externe pour verifier la stabilité du document à signer
FMT_MSA.1/Signer agreement to sign an instable document	L'utilisateur doit donner son accord pour signer un document non stable
FMT_SMF.1/Getting signer agreement to sign an instable document	L'utilisateur doit donner son accord pour signer un document non stable
Interaction avec le signataire	
FDP_ITC.1/explicit signer agreement	L'accord explicite du signataire est obligatoire.

Exigences	Argumentaire de couverture
FDP_ROL.2/Abort of the signature process	L'utilisateur peut interrompre l'opération de signature.
Opérations cryptographiques pour la signature	
FCS_COP.1/hash	Calcul de l'empreinte d'un document à faire signer par le SCDev
Transfert des données à signer au SCDev	
FDP_IFC.1/Signature generation	Les données à signer sont transferees au SCDev sous certaines conditions
FDP_IFF.1/Signature generation	
Récupération de la signature électronique	
FDP_IFC.1/Electronic signature export	La TOE peut récupérer la signature générée par le SCDev et l'exporter
FDP_IFF.1/Electronic signature export	
FDP_ETC.2/Electronic signature export	La TOE peut récupérer la signature générée par le SCDev et l'exporter
FMT_MSA.3/Electronic signature export	La signature exportée par la TOE n'est pas modifiable
FMT_MSA.1/SCDev signature generation status	Le statut de l'opération de signature réalisée par le SCDev n'est pas altérable
FMT_SMF.1/Getting SCDev's signature generation status	Le statut de l'opération de signature réalisée par le SCDev est récupérable
Standard	
FPT_TDC.1/Electronic signature	Utilisation des standards CMS, XML/DSIG, XADES-T
FPT_TDC.1/Time reference	Utilisation des standards RFC-3161
FPT_TDC.1/Certificates	Utilisation des standards X509 v3 standard
FPT_TDC.1/Certificat revocation data	Utilisation des standards CRL V2
Présentation des documents au signataire	
FMT_MTD.1/Document format/viewer association table	L'administrateur peut modifier le choix de l'application à utiliser pour visionner les documents
FMT_SMF.1/Management of the document /format association table	L'administrateur peut modifier le choix de l'application à utiliser pour visionner les documents
FMT_MTD.1/viewer activation parameter	L'administrateur peut modifier le parametre d'activation du visualiseur.
FMT_SMF.1/Management of the viewer activation parameter	L'administrateur peut modifier le parametre d'activation du visualiseur.

7.1.3 Fonctions de vérification de signature

F.Vérification_Signature

Cette fonction permet de réaliser une vérification de signature d'un fichier dans le format CMS, XMLSIG ou XADES et d'extraire le document d'origine.

Elle prend en entrée les paramètres suivants :

- Un document signé.
- La politique de signature à appliquer.

Ces paramètres sont selectionnés via l'interface applicative de la TOE ou via les informations fournies au SDK par une application appelante.

Elle effectue une vérification cryptographique de la signature attachée au document en entrée.

Elle extrait les données d'origine.

Elle extrait du document signé le certificat du signataire et effectue une validation de ce certificat selon les règles de validation de la politique de signature.

Elle extrait le ou les jetons d'horodatage présent et applique les règles de vérification de la signature du jeton d'horodatage et de validation du certificat d'horodatage

Elle extrait du document les attributs suivants afin de s'assurer qu'ils respectent les valeurs précisées par la politique de signature :

- Référence de la politique de signature autorisée.
- Type d'engagement autorisé.

- Rôle du signataire autorisé.
- Lieu de signature.

Elle présente un rapport de vérification comprenant les attributs signés, les caractéristiques du document et des informations sur les différentes étapes de la vérification (validation certificat, validation jetons…).

Exigences	Argumentaire de couverture
Récupération de la signature à vérifier	
FDP_IFC.1/Electronic signature	La TOE peut récupérer les données de signature à verifier pour un document
FDP_IFF.1/Electronic signature	
FMT_MSA.3/Electronic signature	Les données de signature à verifier ne sont pas altérables
FMT_MSA.1/Electronic signature	Les données de signature à verifier ne sont pas altérables
FDP_ITC.2/Electronic signature	La TOE peut demander à une application externe de verifier la stabilité du document avant de verifier sa signature
Standard	
FPT_TDC.1/Electronic signature	Utilisation des standards CMS, XML/DSIG, XADES-T
FPT_TDC.1/Time reference	Utilisation des standards RFC-3161
FPT_TDC.1/Certificates	Utilisation des standards X509 v3 standard
FPT_TDC.1/Certificat revocation data	Utilisation des standards CRL V2
Opérations cryptographiques pour la vérification	
FCS_COP.1/Signature verification	Opération de verification de la signature
Export des résultats de la vérification	
FDP_IFC.1/Electronic signature validation	La TOE permet de récupérer les resultats de l'opération de verification de signature
FDP_IFF.1/Electronic signature validation	
FMT_MSA.3/Signature validation status	Personne ne peut altérer les resultats de l'opération de verification de signature
FMT_MSA.1/Signature validation status	Personne ne peut altérer les resultats de l'opération de verification de signature
FDP_ETC.2/Verification status	La TOE permet d'exporter les resultats de l'opération de verification de signature
Récupération d'une base de temps fiable	
FDP_IFC.1/Time reference	La TOE permet d'importer une base de temps fiable
FDP_IFF.1/Time reference	
FMT_MSA.3/Time reference	L'horologe de reference n'est pas altérable
FMT_MSA.1/Time reference	L'horologe de reference n'est pas altérable
FDP_ITC.2/Time reference	La TOE permet d'importer une base de temps fiable
Vérification du chemin de certification	
FMT_MSA.1/Certificate	Le chemin de certification n'est pas modifiable dans les certificats importés
FMT_MSA.1/Certificate validation data	Le chemin de certification n'est pas modifiable dans les données de validation des certificats importés
FDP_IFC.1/Certification path	La TOE peut vérifier le chemin de certification d'un certificat
FDP_IFF.1/Certification path	
FMT_MSA.3/Certification path	Les paramètres de vérification du chemin de certification ne sont pas altérables
FDP_ITC.2/Certification path	La TOE peut récupérer les données necessaries à la verification du chemin de certification

7.1.4 Fonctions de chiffrement/déchiffrement

F.Chiffrement

Cette fonction permet de réaliser le chiffrement dans le format CMS ou XML_Enc d'un ou des documents sélectionnés.

Elle prend en entrée les paramètres suivants :

- Un ou des documents à chiffrer.
- La politique de chiffrement à appliquer.

Ces paramètres sont selectionnés via l'interface applicative de la TOE ou via les informations fournies au SDK par une application appelante.

Elle réalise la suite d'opérations suivantes :

Elle extrait de la politique de chiffrement les informations suivantes :

- Algorithme de chiffrement à utiliser.
- Règles de validation des certificats de chiffrement.

Elle demande à l'utilisateur de sélectionner le ou les certificats de chiffrement des destinataires et procède à leur validation si la politique le demande.

Elle génère logiciellement une clé secrète via un KeyStore Java.

Elle crée une enveloppe chiffrée CMS ou XML_Enc contenant les données chiffrées par la clé secrète, les clés secrètes chiffrées par les certificats de chiffrement et les certificats de chiffrement des destinataires.

Le document chiffré ainsi généré est alors fourni à l'utilisateur ou à l'application appelante via le SDK.

Exigences	Argumentaire de couverture
Sélection de la politique à appliquer	
FMT_MTD.1/Selection of the applied policy	L'utilisateur peut sélectionner la politique qu'il souhaite utiliser pour signer ou chiffrer.
FMT_SMF.1/Selection of the applied policy	L'utilisateur peut sélectionner la politique qu'il souhaite utiliser pour signer ou chiffrer.
FMT_MSA.1/Attributes	L'utilisateur peut sélectionner certains attributs de la politique qu'il souhaite utiliser pour signer ou chiffrer.
FMT_SMF.1/Modification of attributes	L'utilisateur peut sélectionner certains attributs de la politique qu'il souhaite utiliser pour signer ou chiffrer.
Vérification du chemin de certification	
FMT_MSA.1/Certificate	Le chemin de certification n'est pas modifiable dans les certificats importés
FMT_MSA.1/Certificate validation data	Le chemin de certification n'est pas modifiable dans les données de validation des certificats importés
FDP_IFC.1/Certification path	La TOE peut vérifier le chemin de certification d'un certificat
FDP_IFF.1/Certification path	
FMT_MSA.3/Certification path	Les paramètres de vérification du chemin de certification ne sont pas altérables
FDP_ITC.2/Certification path	La TOE peut récupérer les données necessaries à la verification du chemin de certification
Opérations cryptographiques pour le chiffrement	
FCS_COP.1/Encryption	Opération de chiffrement
FCS_CKM.1/Encryption session keys	Génération des clés de session
FCS_CKM.4/Encryption session keys	Destruction sécurisée des clés de session générées
Standard	
FPT_TDC.1/Encryption	Utilisation des standards CMS, XML_Enc
FPT_TDC.1/Certificates	Utilisation des standards X509 v3 standard
FPT_TDC.1/Certificat revocation data	Utilisation des standards CRL V2

F.Déchiffrement

Cette fonction permet de réaliser le déchiffrement dans le format CMS ou XML_Enc d'un ou des documents sélectionnés.

Elle prend en entrée les paramètres suivants :

- Un ou des documents à déchiffrer.
- La politique de déchiffrement à appliquer.

Ces paramètres sont selectionnés via l'interface applicative de la TOE ou via les informations fournies au SDK par une application appelante.

Elle réalise la suite d'opérations suivantes :

Elle extrait de la politique de chiffrement les informations suivantes :

- Règles de validation du certificat de chiffrement.

Elle demande à l'utilisateur de sélectionner le certificat de déchiffrement parmi ceux présents sur le SCDEV puis de s'authentifier pour accéder aux informations du SCDEV par appel à la fonction Authentification.

A partir du certificat de chiffrement fourni par le SCDEV, elle vérifie que ce certificat de chiffrement est référencé dans les données CMS chiffrées.
Si la politique de chiffrement le précise, elle procède à une validation du certificat de chiffrement sélectionné.
Elle procède ensuite au déchiffrement de la clé secrète chiffrée associée en la transférant au SCDEV et en demandant au SCDEV d'utiliser la clé privée correspondant au certificat de chiffrement séléctionné.
Elle procède ensuite au déchiffrement des données CMS ou XML_Enc à partir de la clé secrète déchiffrée fourni par le SCDEV.

Le document « en clair » ainsi généré est alors fourni à l'utilisateur ou à l'application appelante via le SDK.

Exigences	Argumentaire de couverture
Selection du certificat de l'utilisateur	
FDP_IFC.1/User's certificate import	L'utilisateur peut selectionner son certificat à utiliser
FDP_IFF.1/ User's certificate import	
FMT_MSA.3/ User's certificate import	L'utilisateur peut selectionner son certificat à utiliser
FMT_MSA.1/ User's certificate	L'utilisateur peut selectionner son certificat à utiliser
FDP.ITC.2/ User's certificate	L'utilisateur peut selectionner son certificat à utiliser
FPT_TDC.1/ User's Certificate	L'utilisateur peut selectionner son certificat à utiliser
FMT_SMF.1/ User's certificat selection	L'utilisateur peut selectionner son certificat à utiliser
Opérations cryptographiques pour le déchiffrement	
FCS_COP.1/Decryption	Opération de déchiffrement
FCS_CKM.4/Encryption session keys	Destruction sécurisée des clés de session générées
Standard	
FPT_TDC.1/Encryption	Utilisation des standards CMS, XML_Enc

7.1.5 Fonctions de gestion des politiques de signature/chiffrement

F.Signature fichiers de configuration

Cette fonction permet de réaliser indirectement l'authentification de l'administrateur sécurité avant toute action de gestion des politiques. En fait, l'administrateur signe les fichiers de configuration à l'aide d'une application hors de la TOE ; cette signature est vérifiée lors de l'import de ces fichiers dans la TOE, permettant de s'assurer que c'est bien l'administrateur sécurité qui importe un nouveau fichier de configuration.

Exigences	Argumentaire de couverture
Authentification de l'administrateur	
FIA_UAU.1/Administrator authentication	Seules les operations de selection des visualiseur de documents et de sélection de certains parameters autorisés par la politique appliqués sont accessibles sans authentification

F.TS_Gestion_Politique

Cette fonction permet de :

- Visualiser les caractéristiques des politiques disponibles
- Ajouter ou Supprimer des politiques Cette option n'est accessible qu'à l'administrateur de sécurité.
- Sélectionner les politiques applicables.

Exigences	Argumentaire de couverture
Gestion des politiques	
FMT_MTD.1/Management of the policies	La TOE permet à l'administrateur d'ajouter ou de supprimer des politiques
FMT_SMF.1/Management of the signature policies	La TOE permet à l'administrateur d'ajouter ou de supprimer des politiques

7.1.6 Fonctions d'administration et de configuration

F.Gestion_Supports_clés

Cette fonction permet de gérer les paramètres relatifs aux composants externes à la TOE qui contiennent les clés secrètes et les données d'authentification tels que:

- SCDEV (paramétrages librairie PKCS#11 à invoquer, type (PKCS#11, PKCS#12)…)

Exigences	Argumentaire de couverture
Gestion des rôles	
FMT_SMR.1	La TOE doit permettre de gérer les roles

7.2 Couverture des exigences fonctionnelles

Les argumentaires de couverture sont directement disponibles au chapitre 7.1.

VERSIONS SUCCESSIVES

Vers.	*Date*	*Émetteur*	*Vérificateur*	*Approbateur*	*Motif*
2.0	01/06/2010	F.Caro/C.Blad	JF.Wiorek	JF.Wiorek	Mise à jour version TOE.
1.0	07/05/2008	F.Caro	JF.Wiorek	JF.Wiorek	Version déposée pour le dossier d'évaluation. Suppression des références à la qualification.

FICHIERS

Progiciels	*Fichiers utilisateur*	
Windows XP		
Word 2000	*Modèle* *Document :*	Modele ST2-3 ed3.dot TrustySign_FR_CibleSecurite_rev2.0.doc du 30/04/2010

DIFFUSION

P.Nom	*Entité*	*P.Nom*	*Entité*

Ce document est mis à disposition sous forme informatique sur serveur.
Il n'est donc pas formellement diffusé sous forme papier.
En cas d'utilisation d'un exemplaire imprimé de ce document, veuillez vous assurer, en consultant le serveur approprié, que vous disposez bien de la dernière version applicable.