Agence nationale de la sécurité des systèmes d'information

Profil de protection
Application de création de signature électronique

Date d'émission	**:**	2 mars 2011
Référence	**:**	PP-ACSE-CCv3.1
Version	**:**	1.7

Profil de protection enregistré et certifié par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) sous la référence ANSSI-CC-PP-2008/05-M01.

Table des matières

Table des tableaux

1 Introduction

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

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

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

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

1.1 Identification

Élément	Valeur
Titre	Profil de protection – Application de création de signature électronique
Auteurs	Trusted Labs
Version CC	V3.1 Révision 2
Référence	PP-ACSE-CCv3.1
Numéro de version	1.7
Mots clé	Signature électronique, Application de signature électronique, Application de création de signature électronique

Tableau 1 Identification du profil de protection

1.2 Présentation générale du profil de protection

Le présent profil de protection a été élaboré sous l'égide de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) afin de faciliter la certification d'applications de création de signature utilisables notamment dans le cadre du développement de l'administration électronique.

Ce profil de protection est conforme aux préconisations de l'ANSSI pour la qualification de produits de sécurité au niveau standard. En mettant ce profil de protection à la disposition des fournisseurs de produits, l'ANSSI souhaite donc encourager la qualification d'applications de signature sur la base du présent profil.

Ce profil de protection définit des exigences de sécurité pour une application de création de signature pouvant s'interfacer avec un dispositif sécurisé de création de signature électronique (SSCD) ou un dispositif de création de signature (SCDev).

Bien que la certification de l'application de création de signature ne soit pas requise pour bénéficier de la présomption de fiabilité au sens du décret n°2001-272 du 30 mars 2001, il est recommandé de recourir à une telle certification afin d'améliorer la sécurité de l'ensemble

de la chaîne de signature et de disposer de preuves complémentaires en cas de contestation de la signature démontrant que le procédé de signature utilisé n'est pas fiable (c'est à dire en cas d'apport par un tiers contestataire d'une preuve contraire remettant en cause la présomption de fiabilité de la signature).

Le présent profil de protection s'inspire du [CWA 14170]. Il définit les exigences de sécurité d'une application de création de signature électronique. On entend par « création de signature électronique » la génération de la signature d'un document et d'attributs afférents à la signature avec une clé privée associée à un certificat propre au signataire et confinée dans un dispositif de création de signature (dénommé par la suite *SCDev*).

L'application de création de signature permet de créer au mieux des signatures électroniques présumées fiables[1], et au moins des signatures électroniques sécurisées[2]. Pour permettre cette modularité d'utilisation, l'utilisation de certificats qualifiés et d'un dispositif sécurisé de création de signature (SSCD) n'est pas exigée dans ce document.

Les calculs cryptographiques mettant en œuvre la clé privée du signataire et permettant ainsi de créer la signature sont réalisés dans un dispositif de création de signature (dénommé SCDev[3]) et non dans l'application visée dans le présent profil de protection.

1.3 Définitions et acronymes

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

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

1.4 Références

1.4.1 Références normatives

[CC1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 3.1, Revision 1, September 2006.
[CC2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements. Version 3.1, Revision 2, September 2007.
[CC3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements. Version 3.1, Revision 2, September 2007.
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology. Version 3.1, Revision 2, September 2007.
[QUA-STD]	Processus de qualification d'un produit de sécurité – Niveau standard. Version 1.2 voir www.ssi.gouv.fr.

[1] Signatures électroniques qualifiées au sens de la Directive.
[2] Signatures électroniques avancées au sens de la Directive.
[3] Le dispositif de création de signature (SCDev) est aussi dénommé SSCD, lorsqu'il est évalué conformément aux critères définis dans l'annexe III de la Directive. Le profil de protection défini dans le [[CWA 14169] est reconnu comme étant conforme à ces critères.

1.4.2 Références informatives

[Directive]	Directive européenne sur la signature électronique, 13 décembre 1999, 1999/93/CE.
[CRYPT-STD]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques. ANSSI. voir www.ssi.gouv.fr
[AUTH-STD]	Authentification - Règles et recommandations concernant les mécanismes d'authentification. ANSSI. voir www.ssi.gouv.fr
[CWA 14169]	Secure signature-creation devices “EAL 4+”, CEN/WS, Mars 2004.
[CWA 14170]	Security requirements for signature creation applications, CEN/WS, Mai 2004.
[CWA 14171]	General guidelines for electronic signature verification, CEN/WS, Mai 2004.
[TS 101 733]	Electronic signature formats, ETSI standard, version 1.5.1, 15 décembre 2003.

2 Description de la cible d'évaluation

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

2.1 Description de la TOE

La cible d'évaluation (TOE) est un ensemble de composants logiciels et/ou matériels permettant de créer des signatures électroniques en s'appuyant sur un SCDev effectuant les calculs cryptographiques mettant en œuvre la clé privée du signataire.

La TOE comporte les briques fonctionnelles suivantes :

- Composant gérant l'interaction avec le signataire
- Composant gérant l'invariance de la sémantique du document
- Composant de lancement d'applications de visualisation
- Composant de visualisation des attributs de la signature
- Composant gérant/appliquant les politiques de signature
- Composant formatant et hachant les données à signer
- Composant de pilotage de l'interface avec le SCDev

2.1.1 Composant gérant l'interaction avec le signataire

La TOE comporte une interface avec le signataire, utilisateur de la TOE souhaitant signer un ou plusieurs documents.

Cette interface est soit une interface homme-machine permettant au signataire d'interagir directement avec la TOE, soit une interface programmatique (API) permettant à un composant logiciel (application, bibliothèque...) de jouer le rôle d'interface entre le signataire et la TOE.

Cette interface permet au signataire de :

- Sélectionner/désélectionner un ou plusieurs documents à signer (comprenant ou non déjà une signature)
- Sélectionner la politique de signature appliquée
  Si la TOE supporte plusieurs politiques de signature, la politique de signature à appliquer peut être sélectionnée par le signataire ou résulter d'un paramétrage de l'application.
- Sélectionner les attributs de la signature
- Sélectionner le certificat (et donc la clé privée) à utiliser pour la signature
- Exprimer son consentement à signer
- Activer la clé de signature
- Interrompre le processus de création de signature à tout instant, avant envoi des données à signer au SCDev

La saisie des données d'authentification du signataire permettant au SCDev d'activer la clé de signature et leur transfert vers le SCDev sont sous le contrôle d'un composant extérieur à la TOE.

2.1.1.1 Sélection/désélection des documents à signer

La TOE supporte un moyen permettant au signataire de lui indiquer le ou les documents qu'il souhaite signer.

Document à signer et contre-signature

Le document à signer peut ou non déjà contenir des signatures.

Dans la suite du profil de protection, on désignera comme *document* soit un document simple, soit un document et une ou plusieurs signatures électroniques imbriquées associées, ce second cas revenant à contre-signer le document.

Signature de un ou plusieurs documents

Dans le cas où la signature porte sur plusieurs documents, les mêmes attributs de signature sont utilisés ; en particulier :

- L'identification du certificat du signataire (donc la même clé privée)
- La même politique de signature
- Le même type d'engagement
- La même date présumée
- Etc...

Dans ce cas, une seule interaction non triviale permettra au signataire de signer l'ensemble des documents sélectionnés. Une interaction non triviale peut par exemple être réalisée via un mécanisme de commande/confirmation (le signataire clique sur le bouton signer, la TOE lui demande une confirmation avant exécution de la commande).

Désélection de documents

De plus, après avoir consulté un document qu'il avait sélectionné, le signataire peut refuser de le signer. La TOE lui permet ainsi de désélectionner un ou plusieurs documents déjà sélectionnés.

2.1.1.2 Sélection des attributs de signature

La TOE offre un moyen permettant au signataire de sélectionner les attributs de signature à signer conjointement avec le document.

Les attributs de la signature peuvent être les suivants (la liste n'est pas exhaustive) :

- la référence à la politique de signature,
- le type d'engagement,
- le lieu présumé de la signature,
- la date et l'heure présumées de la signature,
- format du contenu;
- rôle déclaré du signataire
- …

2.1.1.3 Sélection du certificat à utiliser

La TOE supporte un moyen permettant au signataire d'indiquer quel certificat (et donc quelle clé privée) utiliser pour créer la signature.

2.1.1.4 Expression du consentement à signer

L'interface avec le signataire permet à celui-ci d'exprimer son consentement pour signer et ce pour chacun des documents à signer.

Avant de lancer le processus de signature sur un ou plusieurs documents, la TOE identifie que le signataire souhaite réellement signer et que cela n'est pas le fruit d'une action involontaire ou accidentelle. Pour cela, elle oblige le signataire à réaliser une suite d'opérations non triviales.

L'expression du consentement à signer se différencie de l'opération d'authentification du signataire auprès du SCDev pour qu'il active la clé privée associée au certificat sélectionné ; c'en est un préalable.

2.1.1.5 Interruption du processus de signature

La TOE permet au signataire d'interrompre le processus de signature d'un ou plusieurs documents à tout instant jusqu'au moment où la TOE transmet les données à signer au SCDev.

2.1.2 Problématique "What You See Is What You Sign"

Comme dans le « monde papier », le signataire doit pouvoir consulter les éléments sur lesquels il va s'engager avant de les signer.

Dans ce profil de protection, cette problématique est traitée en trois parties :

1) la TOE permet au signataire de visualiser le document à signer grâce au composant de lancement d'applications de visualisation externes (cf. section 2.1.2.1).

2) Contrairement aux documents papier, la sémantique des documents électroniques peut dans certains cas changer en fonction de l'environnement dans lequel ils sont visualisés. La TOE participe au contrôle de l'invariance des documents à signer (cf. section 2.1.2.2).

3) Enfin, la TOE permet au signataire de visualiser les attributs qui seront signés conjointement avec le document, grâce au composant de visualisation des attributs de signature (cf. section 2.1.2.3)

2.1.2.1 Composant de lancement d'applications de visualisation

Le signataire doit être en mesure d'apprécier le contenu du document électronique au moment de la création de la signature électronique.

La TOE doit permettre, sur demande du signataire, le lancement d'une application de présentation correspondant au format du document à visualiser. Ce format est fourni à la TOE directement par l'utilisateur, ou est validé par l'utilisateur.

Pour ce faire, la TOE gère la correspondance entre les formats de document qu'elle accepte et des applications de visualisation. Les applications de visualisation que la TOE lance sont

définies par l'administrateur de la TOE. Ces applications de visualisation sont en dehors du périmètre de la TOE.

Note d'application :

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

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

2.1.2.2 Composant gérant l'invariance de la sémantique du document

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

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

D'autre part, le vérificateur qui recevra la signature peut aussi être induit en erreur. Celui-ci pourrait en effet être amené à visualiser un document sémantiquement différent de celui présenté au signataire.

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

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

La TOE est chargée d'informer le signataire dans le cas où le module externe décèle que la sémantique du document n'est pas stable ou qu'elle ne peut être contrôlée.

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.

Note d'application :

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

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

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

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

2.1.2.3 Composant de visualisation des attributs de la signature

La TOE permet au signataire de visualiser les attributs de signature sélectionnés avant d'engendrer la signature.

2.1.3 Composant gérant/appliquant les politiques de signature

Une politique de signature est un ensemble de règles pour la création ou la validation d'une signature électronique, suivant lesquelles une signature peut être déterminée valide.

Au moment de la création de la signature, un sous-ensemble de la politique de signature doit être mis en œuvre. Ce sous-ensemble définit les exigences minimales requises pour que la signature puisse être acceptée.

Parmi ces exigences, on peut trouver des exigences sur le certificat du signataire telles que :

- Une liste d'identifiants de politiques de certification acceptables pour le signataire ;
- Des informations concernant les usages de la clé privée (*key usage*) ;
- Des extensions requises pour le certificat (*QCstatements*).

On peut par ailleurs trouver des exigences portant sur d'autres attributs :

- Les types d'engagement autorisés pour cette politique
- ...

La TOE doit supporter l'une des deux alternatives suivantes :

- Elle utilise une ou plusieurs politiques de signature stockées sous forme de code exécutable (politiques fixes)
- Elle utilise des politiques de signature sous forme de fichiers interprétables par la TOE (politiques paramétrables)

2.1.4 Composant formatant/hachant les données à signer

Ce composant formate les données à signer ainsi que les attributs de la signature et produit ainsi une représentation des données à signer (DTBSR). Celui-ci peut prendre la forme

- d'un condensé formaté de la totalité des données à signer ;
- ou d'un condensé intermédiaire correspondant à une partie des données à signer associé au complément des données à signer ;
- ou de la totalité des données à signer.

2.1.5 Composant de pilotage de l'interface avec le SCDev

Pour pouvoir interagir avec le SCDev, le composant de pilotage utilise des composants logiciels et/ou matériels intermédiaires (*middleware*). Ces composants intermédiaires sont hors du périmètre de la TOE.

Le composant de pilotage de l'interface avec le SCDev assure les fonctions suivantes :

- Obtenir du SCDev les références des certificats utilisables par le signataire, ou les certificats eux-mêmes ;
- Indiquer au SCDev la clé de signature à activer ;
- Transférer au SCDev la représentation des données à signer ;

- Pour chaque document à signer, recevoir du SCDev la signature numérique ainsi que les statuts d'exécution relatifs à la bonne ou à la mauvaise terminaison du processus de création de signature ;
- Vérifier la conformité de la signature numérique vis-à-vis des données à signer,
- Gérer (refermer) une session avec le SCDev.

Note : Le terme « session » est défini ici comme « la période de temps pendant laquelle la clé privée du signataire est activée dans le SCDev et où celui-ci peut engendrer des signatures. Une session commence dès que le signataire s'est correctement authentifié auprès du SCDev (via la TOE) pour utiliser un couple clé privée/certificat donné. Elle se termine lorsque la TOE la ferme explicitement. »

Note : La vérification de la conformité de la signature numérique doit être faite vis-à-vis des données à signer. En particulier, lorsque le SCDev réalise tout ou partie du hachage des données à signer, la TOE devra vérifier la conformité du condensé retournée par le SCDev. Lorsque la représentation des données à signer envoyé par la TOE au SCDev consiste en un condensé, la vérification de la conformité de la signature numérique pourra se faire vis-à-vis du condensé transmis.

2.2 Environnement d'utilisation de la TOE

L'application de création de signature électronique 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 (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).
- Un logiciel permettant de présenter le document au signataire et l'alertant si ses caractéristiques ne sont pas complètement compatibles avec les caractéristiques d'affichage requises par le document (utilisation de couleur, présence des polices nécessaires, …).
- Un composant logiciel et/ou matériel contrôlant l'invariance de la sémantique du document (vérifie que sa sémantique ne dépend pas de paramètres qui lui sont extérieurs).
- 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).

3 Déclarations de conformité

Ce chapitre contient les sections suivantes :

3.1 Déclaration de Conformité aux CC

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

Il a été écrit conformément aux:

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

3.2 Déclaration de conformité à un Paquet

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

3.3 Déclaration de conformité du PP

Ce PP ne déclare de conformité à aucun autre PP.

3.4 Déclaration de conformité au PP

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

4 Définition du problème de sécurité

4.1 Biens

Cette section décrit l'ensemble des biens à protéger par la TOE.

4.1.1 Biens à protéger par la TOE (User data)

Cette section présente les biens de l'utilisateur (le signataire) qui doivent être protégés par la TOE.

4.1.1.1 Document à signer

B.Ensemble_Des_Documents_A_Signer

L'ensemble des documents à signer lors de l'invocation du processus de signature peut être composé de:

- soit un unique document électronique
- soit plusieurs documents électroniques

Protection: intégrité, confidentialité

Note d'application

Comme on l'a vu à la section 2.1.1.1, on entend ici par document:

- soit simplement un document électronique;
- soit un document électronique avec une ou plusieurs signatures imbriquées attachées au document.

4.1.1.2 Représentations des données à signer

Les biens suivants correspondent à plusieurs représentations successives des données à signer.

Elles requièrent une protection en intégrité.

B.Données_A_Signer

Les données à signer sont les informations sur lesquelles portera la signature.

Elles comprennent:

- Le document à signer
- Les attributs de la signature sélectionnés par le signataire explicitement ou implicitement par l'application.

Les attributs de la signature *doivent* comporter les données suivantes:

- Le certificat du signataire ou une référence non ambiguë de ce certificat

Ils *peuvent* comporter:

- La référence à la politique de signature,
- Le type d'engagement,
- Le lieu présumé de la signature,
- La date et l'heure présumées de la signature,

- Le format du contenu
- …

Protection: intégrité, confidentialité

B.Données_A_Signer_Formatées

Ces données correspondent à un premier formatage des données à signer (enveloppe).

Protection: intégrité, confidentialité

B.Condensé_Des_Données_A_Signer

Cette donnée est un condensé des *données à signer formatées*.

Protection: intégrité

B.Condensé_Formaté

Ce bien correspond au *condensé des données à signer* après avoir subi un formatage, préalablement à son envoi vers le SCDev.

Protection: intégrité

4.1.1.3 Données retournées par la TOE

B.Signature_Électronique

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 à protégé par la TOE au cours de sa constitution avant qu'il soit transmis au signataire.

Protection: intégrité

4.1.2 Biens sensibles de la TOE (TSF data)

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

B.Politique_De_Signature

La TOE réalise la signature selon une politique de signature.

Protection: intégrité

B.Services

Ce bien représente le code exécutable implémentant les services rendus.

Protection: intégrité

B.Correspondances_Entre_Représentations_De_Données

Les données internes à la TOE possèdent souvent une représentation différente de celles présentées au signataire ou entrées dans la TOE.

Ex 1: le type d'engagement (ex: "lu et approuvé") du signataire peut par exemple être représenté en interne par un OID alors qu'il est présenté explicitement au signataire dans l'interface.

Ex 2: le format du document entré dans la TOE peut lui aussi être représenté en interne sous la forme d'un OID.

Protection: intégrité

B.Correspondance_FormatDoc_Application

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

Protection: intégrité

4.2 Sujets

S.Signataire

Le signataire interagit avec la TOE pour signer un ou plusieurs documents selon une politique de signature.

S.Administrateur_De_Sécurité

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

- gestion de la correspondance entre les formats de document autorisés et les applications permettant leur présentation au signataire
- gestion du paramètre de configuration déterminant si la TOE peut signer un document jugé instable.
- dans le cas où la TOE utilise des politiques de signature paramétrables, gestion la liste des politiques de signature utilisables par la TOE.

Note d'application

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

4.3 Menaces

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

4.4 Politiques de sécurité organisationnelles (OSP)

Cette section définit les règles applicables à la TOE.

4.4.1 Politiques relatives à 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:

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

4.4.2 Contrôle de l'invariance de la sémantique du document

P.Sémantique_Document_Invariante

La TOE doit informer le signataire 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:

- o Soit la politique de signature impose de stopper le processus de signature.
- o 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.

4.4.3 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 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 au signataire.

4.4.4 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 l'ANSSI [CRYPT-STD].

4.4.5 Interaction avec le signataire

P.Signature_De_Plusieurs_Document

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

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

P.Arrêt_Processus_Signature

Le signataire 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.

4.4.6 Divers

P.Association_Certificat/Clé_privée

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

P.Export_Signature_Électronique

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: le certificat du signataire in extenso, un tampon d'horodatage, etc.).

P.Administration

La TOE doit permettre à l'administrateur de sécurité de gérer (ajouter/supprimer) les politiques de signature [B.Politique_De_Signature] et la table de correspondance entre les applications de visualisation et les formats de documents en entrée de la TOE [B.Correspondance_FormatDoc_Application].

4.5 Hypothèses

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

4.5.1 Hypothèses sur l'environnement d'utilisation

4.5.1.1 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 du signataire soit sous le contrôle de l'organisation à laquelle le signataire 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.

4.5.1.2 Hypothèses relatives le dispositif de création de signature

Les hypothèses suivantes ont trait au dispositif de création de signature lui-même ou aux différentes interactions possibles de l'environnement de la TOE avec celui-ci.

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.

On suppose de plus qu'il est en charge de l'authentification du signataire pour lui permettre ou non d'utiliser la clé privée correspondant au certificat sélectionné.

Le SCDev est ainsi directement en charge de la protection des données propres au signataire.

Les données suivantes sont supposées être 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, protégées en confidentialité et en intégrité
  - le(s) certificat(s) du signataire, protégés en intégrité, à défaut une référence non ambiguë 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 (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.

Note d'application

L'ensemble des composants assurant la communication entre la TOE et le SCDev peut être composé de différents composants logiciels et/ou matériels installés sur le système d'exploitation (ex: les pilotes PKCS#11 ou des fournisseurs de services cryptographiques (CSP) définissant une interface cryptographique que la TOE appelle pour accéder à un dispositif générant effectivement la signature).

H.Authentification_Signataire

On suppose que les composants logiciels et matériels permettant au signataire de s'authentifier auprès du SCDev pour qu'il active la clé privée de signature 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.

4.5.1.3 Présentation du document

H.Présentation_Du_Document

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

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

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.

4.5.1.4 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 à signer est bien invariante et de communiquer le statut de son analyse à la TOE.

4.5.2 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 utilisables par la TOE est supposée authentique.

4.5.3 Conclusion

Note d'application:

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

5 Objectifs de sécurité

5.1 Objectifs de sécurité pour la TOE

5.1.1 Objectifs généraux

O.Association_Certificat/Clé_privée

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

5.1.2 Interaction avec le signataire

O.Présentation_Conforme_Des_Attributs

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

O.Consentement_Explicite

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

O.Abandon_Du_Processus_De_Signature

La TOE devra fournir les moyens au signataire pour interrompre le processus de signature à tout moment, avant l'activation de la clé de signature.

O.Ensemble_De_Documents_A_Signer

Après que le signataire a donné son consentement pour signature, la TOE devra garantir que l'ensemble des documents effectivement traités correspond exactement à l'ensemble des documents à signer sélectionnés.

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

5.1.3 Application d'une politique de signature

O.Conformité_Du_Certificat

La TOE doit vérifier que le certificat sélectionné par le signataire répond bien aux critères de la politique de signature à appliquer.

O.Validité_Du_Certificat

La TOE devra contrôler que le certificat sélectionné par le signataire est bien utilisé durant sa période de validité.

Note d'application

La référence de temps utilisée pour ce faire est la date fournie par le système d'exploitation de la machine hôte.

O.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.

O.Export_Signature_Électronique

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 facilitant la vérification de la signature peuvent être ajoutées (ex: le certificat du signataire in extenso, un tampon d'horodatage, etc.).

5.1.4 Protection des données

O.Administration

La TOE devra permettre à l'administrateur de sécurité de gérer (ajouter/supprimer) les politiques de signature [B.Politique_De_Signature] et la table de correspondance entre les applications de visualisation et les formats de documents en entrée de la TOE [B.Correspondance_FormatDoc_Application].

5.1.5 Opérations cryptographiques

O.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 seront conformes au référentiel cryptographique de l'ANSSI [CRYPT-STD].

5.1.6 Contrôle de l'invariance de la sémantique du document

O.Contrôle_Invariance_Document

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

La TOE informera le signataire si ce module détermine que la sémantique du document à signer n'est pas stable.

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.

5.1.7 Présentation du ou des documents à signer

O.Lancement_d'Applications_De_Présentation

La TOE devra pouvoir lancer une application externe pour permettre au signataire de visualiser le document à signer.

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.

5.2 Objectifs de sécurité pour l'environnement opérationnel

5.2.1 Machine hôte

OE.Machine_Hôte

La machine hôte sur laquelle la TOE s'exécute devra être soit directement sous la responsabilité du signataire soit sous le contrôle de l'organisation à laquelle le signataire 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.

5.2.2 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 sélectionné.

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 ambiguë 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.

5.2.3 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.

5.2.4 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.

5.2.5 Divers

OE.Contrôle_Sémantique_Document_à_Signer

L'environnement de la TOE devra fournir un module capable de déterminer si la sémantique du document à signer est bien invariante et de 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.

6 Exigences de sécurité

6.1 Exigences de sécurité fonctionnelles

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	**Object / Information**	**Operation**	**Security attributes**
the Signer	a document to be signed	import of the document in the TOE	**the Signer:** - signature policy - signer's explicit agreement to sign the document if is not stable **a document to be signed:** - document's identifier - document's stability status
the Signer	the signer's certificate	import of the signer's certifiifcate into the TOE	**the Signer:** - applied signature policy **the signer's certificate:** - key usage status - QCStatement if required by the signature policy - certificate identifier
- the Signer - the SCDev	- the data to be signed formatted - the electronic signature	transfert to the SCDev	**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

Subject	Object / Information	Operation	Security attributes
- the Signer - the SCDev	the electronic signature	export to the Signer	**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

6.1.1 Contrôle de l'invariance de la sémantique du document

Les exigences définies dans cette section portent sur le contrôle de l'invariance de la sémantique du document signé.

6.1.1.1 Contrôle à l'import du document

FDP_IFC.1/Document acceptance Subset information flow control

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

- **subjects: the signer,**
- **information: a document to be signed**
- **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 signer (signature policy, signer's explicit agreement to sign the document if is not stable)**
- **information: a document to be signed (document's identifier, document's stability status)**
- **operation: import of the document**.

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**.

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

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

- **controls succeed**.
- **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.**

Note d'application

La TOE devra fournir les moyens pour:

- invoquer un vérificateur externe chargé de contrôler l'invariance de la sémantique du document à signer,
- informer le signataire du document si la sémantique n'est pas stable
- demander l'accord explicite du signataire pour poursuivre le processus lorsque la sémantique du document n'est pas stable; la politique de signature permet de contourner le contrôle

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 signer when the document's semantics is not stable**.

Raffinement:

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

Note d'application

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

FMT_MSA.3 / Document's acceptance Static attribute initialisation

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

Raffinement:

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

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

FMT_MSA.1 / 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 identifiers*** to **the signer**.

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**.

Raffinement:

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

Note d'application

La liste de documents à signer ne peut plus changer à partir du moment où le signataire a donné son consentement à signer.

A noter néanmoins qu'il peut stopper le processus de signature à tout moment (voir exigence *FDP_ROL.2/Abort of the signature process*).

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

FMT_MSA.1.1/Document's semantics invariance status [Raffiné éditorialement] The TSF shall enforce the **document acceptance 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 Interaction avec le signataire

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 [Raffiné éditorialement] The TSF shall permit operations to be rolled back **[before the data to be signed formatted are transferred to the SCDev**.

6.1.3 Règles de validation

6.1.3.1 Règles relatives aux attributs de signature

Les exigences qui suivent se rapportent aux attributs de signature.

FMT_MSA.1 / Signature attributes Management of security attributes

FMT_MSA.1.1 / Signature attributes The TSF shall enforce the **signature generation information flow control policy** to restrict the ability to ***select*** the security attributes **signature attributes** to **the signer**.

FMT_SMF.1 / Modification of signature attributes Specification of Management Functions

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

- **permit the signer to change the value of the signature attributes required by the applied signature policy**.

Raffinement:

The TSF shall allow the modification of signature attributes until the signer has given his agreement to sign.

6.1.3.2 Règles relatives au certificat du signataire

Les exigences qui suivent se rapportent aux règles de vérification s'appliquant au certificat du signataire.

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

FDP_IFC.1.1/Signer's certificate import The TSF shall enforce the **signer's certificate information flow control policy** on

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

FDP_IFF.1/Signer's certificate import Simple security attributes

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

- **subjects: the signer (applied signature policy)**
- **information: the signer's certificate (key usage, Signature SFP)**.

FDP_IFF.1.2/Signer'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 if required by the signature policy (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/Signer's certificate import The TSF shall enforce the **other rules explicitly defined in the Signature SFP (eventually including the QCStatement)**.

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/Signer's certificate import The TSF shall explicitly deny an information flow based on the following rules:

- **controls fail**.

FMT_MSA.3/Signer's certificate import Static attribute initialisation

FMT_MSA.3.1/Signer's certificate import The TSF shall enforce the **signer's certificate information flow control policy** to provide ***restrictive*** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/Signer'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/Signer's certificate Management of security attributes

FMT_MSA.1.1/Signer's certificate The TSF shall enforce the **signer's certificate information flow control policy** to restrict the ability to ***select*** the security attributes **certificate identifier** to **the signer**.

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

FDP_ITC.2.1/Signer's certificate The TSF shall enforce the **signer's certificate information flow control policy** when importing user data, controlled under the SFP, from outside of the TOE.

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

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

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

FPT_TDC.1.1/Signer's 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/Signer's certificate The TSF shall use **[assignment: list of interpretation rules to be applied by the TSF]** when interpreting the TSF data from another trusted IT product.

Note d'application

Les rédacteurs de cibles de sécurité devront mentionner les standards supportés par le produit.

FMT_SMF.1/Signer's certificate selection Specification of Management Functions

FMT_SMF.1.1/Signer's 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 policy**.

6.1.4 Application de la politique de signature et génération de la signature numérique

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 electronic 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, [assignment: any other signer's attribute]), signer's explicit agreement to sign the present non invariant document (see *FDP_IFF.1.2/Signature generation*, the SCDev ([assignment: SCDev's attribute])**

- **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, [assignment: list of supported signature attributes])**.

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;**
- **[assignment: any other supported rule on signature attributes]**.

FDP_IFF.1.3/Signature generation The TSF shall enforce the **the others rules explicitly defined in the applied signature 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**.

Note d'application

La TOE doit fournir les moyens de:

- Communiquer les attributs de signature au signataire avant la génération de signature
- Lancer la visionneuse correspondante au format du document, selon la table d'association "format/ viewer"
- Activer la clé de signature correspondante au sélectionnement de certificat du signataire

Note that the conformance of the signer's certificate with respect to the applied signature policy is not check in the present policy but in the *signer's certificate information flow control policy* that is the subject of component *FDP_IFC.1/Signer's certificate import*. In the present component the conformance of the signer's certificate is assumed established.

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

FDP_ITC.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: **[assignment: additional importation control rules]**.

Note d'application

FDP_ITC.1.3: Les rédacteurs de cibles de sécurité devront préciser la suite d'événements que la TOE devra observer pour considérer que le signataire donne effectivement son agrément pour signer.

6.1.5 Retour 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 electronic signature**
- **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 ([assignment: signer's security attributes])**
  - **the SCDev (the status of signature generation process, [assignment: any other SCDev attributes])**
- **information:**
  - **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, [assignment: 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: **[assignment: 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 [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/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)**.

6.1.6 Opération cryptographiques

FCS_COP.1 / Hash function Cryptographic operation

FCS_COP.1.1 / Hash function The TSF shall perform

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

Note d'application:

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

6.1.7 Identification et authentification de l'utilisateur

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles

- **the signer**
- **the security administrator**.

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

FIA_UID.2 User identification before any action

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

Note d'application

Le mécanisme d'authentification doit être conforme au référentiel d'authentification de l'ANSSI [AUTH-STD].

6.1.8 Administration de la TOE

6.1.8.1 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/viewer association table Specification of Management Functions

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

- **allow the administrator of the TOE to manage [assignment: management operations] the document format/viewer association table**.

Note d'application

Dans "l'assignment", les rédacteurs de cibles doivent définir les opérations que la TOE autorise l'administrateur de réaliser sur la table d'association entre les formats de document et les visualisateurs. Les opérations possibles peuvent être l'ajout de nouvelles entrées dans cette table, la suppression d'entrées, la modification de l'application de visualisation, etc...

6.1.8.2 Gestion des politiques de signature

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

FMT_MTD.1.1 / Management of the signature policies The TSF shall restrict the ability to ***[assignment: list of allowed management operations]*** the **signature policies** to **the security administrator of the TOE**.

Note d'application

Ce composant fonctionnel doit être instancié de manière cohérente avec le composant *FMT_SMF.1/Management of the signature policies*.

FMT_SMF.1 / Management of the signature policies Specification of Management Functions

FMT_SMF.1.1 / Management of the signature policies The TSF shall be capable of performing the following management functions: **[assignment: list of management functions to be provided by the TSF]**.

Note d'application

Ce composant fonctionnel doit être instancié de manière cohérente avec le composant *FMT_MTD.1/Management of the signature policies*.

6.2 Exigences de sécurité d'assurance

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

7 Argumentaires

7.1 Objectifs de sécurité / problème de sécurité

7.1.1 Politiques de sécurité organisationnelles (OSP)

7.1.1.1 Politiques relatives à la validité de la signature créée

P.Conformité_Certificat_Signataire Cette politique est couverte par l'objectif *O.Conformité_Du_Certificat* qui requiert que la TOE contrôle la conformité du certificat sélectionné par le signataire vis-à-vis des exigences de la politique de signature.

P.Validité_Certificat_Signataire Cette politique est couverte par l'objectif *O.Validité_Du_Certificat* qui requiert que la TOE contrôle que le certificat sélectionné par le signataire est bien en cours de validité.

P.Conformité_Attributs_Signature Cette politique est couverte par l'objectif *O.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.

7.1.1.2 Contrôle de l'invariance de la sémantique du document

P.Sémantique_Document_Invariante La politique de sécurité organisationnelle *P.Sémantique_Du_Document_Invariante* est couverte:

- d'une part par l'objectif de sécurité sur la TOE *O.Contrôle_Invariance_Document* qui requiert que la TOE interroge un module externe chargé de contrôler l'invariance de la sémantique du document signé, 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_à_Signer* qui requiert que l'environnement de la TOE fournisse un tel module.

7.1.1.3 Présentation du document et des attributs de signature au signataire

P.Possibilité_De_Présenter_Le_Document La politique de sécurité est couverte par les objectifs *O.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.

P.Présentation_Attributs_De_Signature Cette politique est couverte totalement par l'objectif *O.Présentation_Conforme_Des_Attributs* qui requiert que la TOE offre au signataire une représentation des attributs de signature conforme à ceux qui seront signés.

7.1.1.4 Conformité aux standards

P.Algorithme_De_Hachage La politique de sécurité organisationnelle est couverte entièrement par l'objectif *O.Operations_Cryptographiques* qui en reprend les termes.

7.1.1.5 Interaction avec le signataire

P.Signature_De_Plusieurs_Document La politique est couverte par l'objectif *O.Ensemble_De_Documents_A_Signer* 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 Cette politique est couverte par l'objectif *O.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 Cette politique de sécurité organisationnelle est couverte par l'objectif *O.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.

7.1.1.6 Divers

P.Association_Certificat/Clé_privée La politique de sécurité organisationnelle *P.Association_Certificat/Clé_privée* est complètement couverte par l'objectif de sécurité *O.Association_Certificat/Clé_privée* qui en reprend les éléments.

P.Export_Signature_Électronique La politique de sécurité organisationnelle est couverte entièrement par l'objectif *O.Export_Signature_Électronique* qui en reprend les termes.

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

7.1.2 Hypothèses

7.1.2.1 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_Signataire 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.

7.1.2.2 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.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.

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

Tableau 2 Association menaces vers objectifs de sécurité

Politiques de sécurité organisationnelles (OSP)	Objectifs de sécurité	Argumentaire
P.Conformité_Certificat_Signataire	O.Conformité_Du_Certificat	Section 7.1.1
P.Validité_Certificat_Signataire	O.Validité_Du_Certificat	Section 7.1.1
P.Conformité_Attributs_Signature	O.Conformité_Des_Attributs	Section 7.1.1
P.Sémantique_Document_Invariante	O.Contrôle_Invariance_Document, OE.Contrôle_Sémantique_Document_à_Signer	Section 7.1.1
P.Possibilité_De_Présenter_Le_Document	O.Lancement_d'Applications_De_Présentation, OE.Présentation_Document	Section 7.1.1
P.Présentation_Attributs_De_Signature	O.Présentation_Conforme_Des_Attributs	Section 7.1.1
P.Algorithme_De_Hachage	O.Operations_Cryptographiques	Section 7.1.1
P.Signature_De_Plusieurs_Document	O.Ensemble_De_Documents_A_Signer	Section 7.1.1
P.Arrêt_Processus_Signature	O.Abandon_Du_Processus_De_Signature	Section 7.1.1
P.Consentement_Explicite	O.Consentement_Explicite	Section 7.1.1
P.Association_Certificat/Clé_privée	O.Association_Certificat/Clé_privée	Section 7.1.1
P.Export_Signature_Électronique	O.Export_Signature_Électronique	Section 7.1.1
P.Administration	O.Administration, OE.Administrateur_De_Sécurité_Sûr	Section 7.1.1

Tableau 3 Association politiques de sécurité organisationnelles vers objectifs de sécurité

Objectifs de sécurité	Politiques de sécurité organisationnelles (OSP)
O.Association_Certificat/Clé_privée	P.Association_Certificat/Clé_privée
O.Présentation_Conforme_Des_Attributs	P.Présentation_Attributs_De_Signature
O.Consentement_Explicite	P.Consentement_Explicite
O.Abandon_Du_Processus_De_Signature	P.Arrêt_Processus_Signature
O.Ensemble_De_Documents_A_Signer	P.Signature_De_Plusieurs_Document
O.Conformité_Du_Certificat	P.Conformité_Certificat_Signataire
O.Validité_Du_Certificat	P.Validité_Certificat_Signataire
O.Conformité_Des_Attributs	P.Conformité_Attributs_Signature
O.Export_Signature_Électronique	P.Export_Signature_Électronique
O.Administration	P.Administration
O.Operations_Cryptographiques	P.Algorithme_De_Hachage
O.Contrôle_Invariance_Document	P.Sémantique_Document_Invariante
O.Lancement_d'Applications_De_Présentation	P.Possibilité_De_Présenter_Le_Document
OE.Machine_Hôte	
OE.Dispositif_De_Création_De_Signature	
OE.Communication_TOE/SCDev	
OE.Protection_Données_Authentification_Signataire	
OE.Présence_Du_Signataire	
OE.Présentation_Document	P.Possibilité_De_Présenter_Le_Document
OE.Contrôle_Sémantique_Document_à_Signer	P.Sémantique_Document_Invariante
OE.Authenticité_Origine_Politique_Signature	
OE.Administrateur_De_Sécurité_Sûr	P.Administration
OE.Intégrité_Services	

Tableau 4 Association objectifs de sécurité vers politiques de sécurité organisationnelles

Hypothèses	Objectifs de sécurité pour l'environnement opérationnel	Argumentaire
H.Machine_Hôte	OE.Machine_Hôte	Section 7.1.2
H.Dispositif_De_Création_De_Signature	OE.Dispositif_De_Création_De_Signature	Section 7.1.2
H.Communication_TOE/SCDev	OE.Communication_TOE/SCDev	Section 7.1.2
H.Authentification_Signataire	OE.Protection_Données_Authentification_Signataire	Section 7.1.2
H.Présentation_Du_Document	OE.Présentation_Document	Section 7.1.2
H.Présentation_Signatures_Existantes	OE.Présentation_Document	Section 7.1.2
H.Contrôle_Invariance_Sémantique_Document	OE.Contrôle_Sémantique_Document_à_Signer	Section 7.1.2
H.Présence_Du_Signataire	OE.Présence_Du_Signataire	Section 7.1.2
H.Administrateur_De_Sécurité_Sûr	OE.Administrateur_De_Sécurité_Sûr	Section 7.1.2
H.Intégrité_Services	OE.Intégrité_Services	Section 7.1.2
H.Politique_Signature_D'Origine_Authentique	OE.Authenticité_Origine_Politique_Signature	Section 7.1.2

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

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_Signataire
OE.Présence_Du_Signataire	H.Présence_Du_Signataire
OE.Présentation_Document	H.Présentation_Du_Document, H.Présentation_Signatures_Existantes
OE.Contrôle_Sémantique_Document_à_Signer	H.Contrôle_Invariance_Sémantique_Document
OE.Authenticité_Origine_Politique_Signature	H.Politique_Signature_D'Origine_Authentique
OE.Administrateur_De_Sécurité_Sûr	H.Administrateur_De_Sécurité_Sûr
OE.Intégrité_Services	H.Intégrité_Services

Tableau 6 Association objectifs de sécurité pour l'environnement opérationnel vers hypothèses

7.2 Exigences de sécurité / objectifs de sécurité

7.2.1 Objectifs

7.2.1.1 Objectifs de sécurité pour la TOE

Objectifs généraux

O.Association_Certificat/Clé_privée L'objectif *O.Association_Certificat/Clé_privée* 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.

Interaction avec le signataire

O.Présentation_Conforme_Des_Attributs L'objectif *O.Présentation_Conforme_Des_Attributs* 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.

O.Consentement_Explicite L'objectif *O.Consentement_Explicite* 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.

O.Abandon_Du_Processus_De_Signature L'objectif *O.Abandon_Du_Processus_De_Signature* 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.

O.Ensemble_De_Documents_A_Signer L'objectif *O.Ensemble_De_Documents_A_Signer* est couvert par les exigences fonctionnelles:

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

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

Application d'une politique de signature

O.Conformité_Du_Certificat L'objectif de sécurité *O.Conformité_Du_Certificat* 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/Signer's certificate import*). Le composant fonctionnel *FDP_IFF.1/Signer'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/Signer's certificate* et *FPT_TDC.1/Signer'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/Signer'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/Signer's certificate* et *FMT_SMF.1/Signer'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.

O.Validité_Du_Certificat L'objectif de sécurité *O.Validité_Du_Certificat* 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/Signer's certificate import*). Le composant fonctionnel *FDP_IFF.1/Signer'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/Signer's certificate* et *FPT_TDC.1/Signer'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/Signer'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/Signer's certificate* et *FMT_SMF.1/Signer'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.

O.Conformité_Des_Attributs L'objectif de sécurité *O.Conformité_Des_Attributs* 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/Signature attributes* et *FMT_SMF.1/Modification of signature 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.

O.Export_Signature_Électronique L'objectif de sécurité *O.Export_Signature_Électronique* 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.

Protection des données

O.Administration L'objectif *O.Administration* 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 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.

Opérations cryptographiques

O.Operations_Cryptographiques L'objectif de sécurité *O.Operations_Cryptographiques* est couvert par l'exigence *FCS_COP.1/Hash function* qui permet aux développeurs de cibles de sécurité de définir les algorithmes de hachages implantés dans la TOE.

Contrôle de l'invariance de la sémantique du document

O.Contrôle_Invariance_Document L'objectif de sécurité *O.Contrôle_Invariance_Sémantique_Du_Document* 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.

Présentation du ou des documents à signer

O.Lancement_d'Applications_De_Présentation L'objectif de sécurité *O.Lancement_d'Applications_De_Présentation* 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.

7.2.2 Tables de couverture entre objectifs et exigences de sécurité

Objectifs de sécurité	Exigences fonctionnelles pour la TOE	Argumentaire
O.Association_Certificat/Clé_privée	FDP_IFF.1/Signature generation	Section 7.2.1
O.Présentation_Conforme_Des_Attributs	FDP_IFF.1/Signature generation	Section 7.2.1
O.Consentement_Explicite	FDP_ITC.1/Explicit signer agreement	Section 7.2.1
O.Abandon_Du_Processus_De_Signature	FDP_ROL.2/Abort of the signature process	Section 7.2.1
O.Ensemble_De_Documents_A_Signer	FMT_MSA.1/Selected documents, FMT_SMF.1/Selection of a list of documents, FMT_MSA.1/Signature attributes, FMT_SMF.1/Modification of signature attributes	Section 7.2.1
O.Conformité_Du_Certificat	FDP_IFC.1/Signer's certificate import, FDP_IFF.1/Signer's certificate import, FDP_ITC.2/Signer's certificate, FPT_TDC.1/Signer's certificate, FMT_MSA.3/Signer's certificate import, FMT_MSA.1/Signer's certificate, FMT_SMF.1/Signer's certificate selection, FMT_SMR.1, FIA_UID.2	Section 7.2.1

Objectifs de sécurité	Exigences fonctionnelles pour la TOE	Argumentaire
O.Validité_Du_Certificat	FDP_IFC.1/Signer's certificate import, FDP_IFF.1/Signer's certificate import, FDP_ITC.2/Signer's certificate, FPT_TDC.1/Signer's certificate, FMT_MSA.3/Signer's certificate import, FMT_MSA.1/Signer's certificate, FMT_SMF.1/Signer's certificate selection, FMT_SMR.1, FIA_UID.2	Section 7.2.1
O.Conformité_Des_Attributs	FDP_IFC.1/Signature generation, FDP_IFF.1/Signature generation, FMT_MSA.3/Signature generation, FMT_MSA.1/Signature attributes, FMT_SMF.1/Modification of signature attributes, FMT_SMR.1, FIA_UID.2	Section 7.2.1
O.Export_Signature_Électronique	FDP_IFC.1/Electronic signature export, FDP_IFF.1/Electronic signature export, FDP_ETC.2/Electronic signature export, FMT_MSA.3/Electronic signature export, FMT_MSA.1/SCDev signature generation status, FMT_SMR.1, FMT_SMF.1/Getting SCDev's signature generation status, FIA_UID.2	Section 7.2.1

Objectifs de sécurité	Exigences fonctionnelles pour la TOE	Argumentaire
O.Administration	FMT_SMF.1/Management of the document format/viewer association table, FMT_MTD.1/Document format/viewer association table, FMT_SMR.1, FMT_MTD.1/Management of the signature policies, FMT_SMF.1/Management of the signature policies	Section 7.2.1
O.Operations_Cryptographiques	FCS_COP.1/Hash function	Section 7.2.1
O.Contrôle_Invariance_Document	FDP_IFC.1/Document acceptance, FDP_IFF.1/Document acceptance, FDP_ITC.1/Document acceptance, FMT_MSA.3/Document's acceptance, FMT_MSA.1/Document's semantics invariance status, FMT_MSA.1/Signer agreement to sign an instable document, FMT_SMR.1, FMT_SMF.1/Getting document's semantics invariance status, FMT_SMF.1/Getting signer agreement to sign an instable document, FIA_UID.2	Section 7.2.1
O.Lancement_d'Applications_De_Présentation	FDP_IFF.1/Signature generation, FMT_MTD.1/Document format/viewer association table, FMT_SMF.1/Management of the document format/viewer association table	Section 7.2.1

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

Exigences fonctionnelles pour la TOE	Objectifs de sécurité
FDP_IFC.1/Document acceptance	O.Contrôle_Invariance_Document
FDP_IFF.1/Document acceptance	O.Contrôle_Invariance_Document
FDP_ITC.1/Document acceptance	O.Contrôle_Invariance_Document
FMT_MSA.3/Document's acceptance	O.Contrôle_Invariance_Document
FMT_MSA.1/Selected documents	O.Ensemble_De_Documents_A_Signer
FMT_SMF.1/Selection of a list of documents	O.Ensemble_De_Documents_A_Signer
FMT_MSA.1/Document's semantics invariance status	O.Contrôle_Invariance_Document
FMT_SMF.1/Getting document's semantics invariance status	O.Contrôle_Invariance_Document
FMT_MSA.1/Signer agreement to sign an instable document	O.Contrôle_Invariance_Document
FMT_SMF.1/Getting signer agreement to sign an instable document	O.Contrôle_Invariance_Document
FDP_ROL.2/Abort of the signature process	O.Abandon_Du_Processus_De_Signature
FMT_MSA.1/Signature attributes	O.Ensemble_De_Documents_A_Signer, O.Conformité_Des_Attributs
FMT_SMF.1/Modification of signature attributes	O.Ensemble_De_Documents_A_Signer, O.Conformité_Des_Attributs
FDP_IFC.1/Signer's certificate import	O.Conformité_Du_Certificat, O.Validité_Du_Certificat
FDP_IFF.1/Signer's certificate import	O.Conformité_Du_Certificat, O.Validité_Du_Certificat
FMT_MSA.3/Signer's certificate import	O.Conformité_Du_Certificat, O.Validité_Du_Certificat
FMT_MSA.1/Signer's certificate	O.Conformité_Du_Certificat, O.Validité_Du_Certificat
FDP_ITC.2/Signer's certificate	O.Conformité_Du_Certificat, O.Validité_Du_Certificat

Exigences fonctionnelles pour la TOE	Objectifs de sécurité
FPT_TDC.1/Signer's certificate	O.Conformité_Du_Certificat, O.Validité_Du_Certificat
FMT_SMF.1/Signer's certificate selection	O.Conformité_Du_Certificat, O.Validité_Du_Certificat
FDP_IFC.1/Signature generation	O.Conformité_Des_Attributs
FDP_IFF.1/Signature generation	O.Association_Certificat/Clé_privée, O.Présentation_Conforme_Des_Attributs, O.Conformité_Des_Attributs, O.Lancement_d'Applications_De_Présentation
FMT_MSA.3/Signature generation	O.Conformité_Des_Attributs
FDP_ITC.1/Explicit signer agreement	O.Consentement_Explicite
FDP_IFC.1/Electronic signature export	O.Export_Signature_Électronique
FDP_IFF.1/Electronic signature export	O.Export_Signature_Électronique
FDP_ETC.2/Electronic signature export	O.Export_Signature_Électronique
FMT_MSA.3/Electronic signature export	O.Export_Signature_Électronique
FMT_MSA.1/SCDev signature generation status	O.Export_Signature_Électronique
FMT_SMF.1/Getting SCDev's signature generation status	O.Export_Signature_Électronique
FCS_COP.1/Hash function	O.Operations_Cryptographiques
FMT_SMR.1	O.Conformité_Du_Certificat, O.Validité_Du_Certificat, O.Conformité_Des_Attributs, O.Export_Signature_Électronique, O.Administration, O.Contrôle_Invariance_Document
FIA_UID.2	O.Conformité_Du_Certificat, O.Validité_Du_Certificat, O.Conformité_Des_Attributs, O.Export_Signature_Électronique, O.Contrôle_Invariance_Document

Exigences fonctionnelles pour la TOE	Objectifs de sécurité
FMT_MTD.1/Document format/viewer association table	O.Administration, O.Lancement_d'Applications_De_Présentation
FMT_SMF.1/Management of the document format/viewer association table	O.Administration, O.Lancement_d'Applications_De_Présentation
FMT_MTD.1/Management of the signature policies	O.Administration
FMT_SMF.1/Management of the signature policies	O.Administration

Tableau 8 Association exigences fonctionnelles vers objectifs de sécurité de la TOE

7.3 Dépendances

7.3.1 Dépendances des exigences de sécurité fonctionnelles

Exigences	Dépendances CC	Dépendances Satisfaites
FDP_ROL.2/Abort of the signature process	(FDP_ACC.1 ou FDP_IFC.1)	FDP_IFC.1/Signature generation
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/Signature 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	
FCS_COP.1/Hash function	(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	
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

Exigences	Dépendances CC	Dépendances Satisfaites
FDP_ITC.1/Document acceptance	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_MSA.3)	FDP_IFC.1/Document acceptance, FMT_MSA.3/Document's acceptance
FMT_MSA.3/Document's acceptance	(FMT_MSA.1) et (FMT_SMR.1)	FMT_SMR.1, FMT_MSA.1/Selected documents, FMT_MSA.1/Document's semantics invariance status
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/Document's semantics invariance status	(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 document's semantics invariance status
FMT_SMF.1/Getting document's semantics invariance status	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/Signature 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/Signer's certificate import
FMT_MSA.3/Signer'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

Exigences	Dépendances CC	Dépendances Satisfaites
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/Document format/viewer association table	(FMT_SMF.1) et (FMT_SMR.1)	FMT_SMR.1, FMT_SMF.1/Management of the document format/viewer association table
FMT_SMF.1/Management of the document format/viewer association table	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	

Tableau 9 Dépendances des exigences fonctionnelles

7.3.1.1 Argumentaire pour les dépendances non satisfaites

La dépendance FCS_CKM.4 de FCS_COP.1/Hash function n'est pas supportée. La dépendance avec FCS_CKM.4 n'est pas satisfaite car la fonction de hachage ne nécessite pas clé cryptographique.

La dépendance FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 de FCS_COP.1/Hash function n'est pas supportée. La dépendance avec FCS_CKM.1, FDP_ITC.1 ou FDP_ITC.2 n'est pas satisfaite car la fonction de hashage ne nécessite pas ni la génération ni l'import de clé dans la TOE.

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:

- 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
- 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.

- enfin, le certificat du signataire, ne nécessite pas de protection en termes de confidentialité.

7.3.2 Dépendances des exigences de sécurité d'assurance

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

Tableau 10 Dépendances des exigences d'assurance

7.3.2.1 Argumentaire pour les dépendances non satisfaites

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

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

7.4 Argumentaire pour l'EAL

Le niveau de ce profil de protection est EAL 3 augmenté, car il est requis par le processus de qualification standard [QUA-STD].

7.5 Argumentaire pour les augmentations à l'EAL

7.5.1 AVA_VAN.3 Focused vulnerability analysis

Augmentation requise par le processus de qualification standard.

7.5.2 ALC_FLR.3 Systematic flaw remediation

Augmentation requise par le processus de qualification standard.

8 Notice

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

Annexe A Glossaire

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

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

A.1 Termes propres aux Critères Communs

Evaluation Assurance Level (EAL)

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

Target Of Evaluation (TOE)

En français, Cible d'évaluation.

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

TOE Security Policy (TSP)

En français, politique de sécurité de la TOE.

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

A.2 Termes propres à la signature électronique

Autorité de certification qualifiée

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

Certificat électronique

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

Un certificat électronique doit comporter :

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

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

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

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

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

f) Le code d'identité du certificat électronique ;

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

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

Certificat électronique qualifié

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

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

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

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

Condensé

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

Cryptographic Service Provider (CSP)

En français, fournisseur de services cryptographiques.

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

Dispositif de création de signature électronique

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

Dispositif sécurisé de création de signature électronique

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

Dispositif de vérification de signature électronique

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

Directive

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

Données de création de signature électronique

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

Données de vérification de signature électronique

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

Format de contenu

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

Object Identifier (OID)

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

Politique de signature

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

Prestataire de services de certification électronique

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

Qualification des prestataires de services de certification électronique

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

Signataire

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

Signature électronique

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

Signature électronique sécurisée

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

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

Signature électronique présumée fiable

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

On parle aussi de signature électronique qualifiée.

Signature numérique

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

Système de création de signature

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

Annexe B Acronymes

ETSI European Telecommunications Standards Institute

CWA CEN Workshop Agreements

CSP Cryptographic Service Provider.

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

SCDev Signature Creation Device

SSCD Secure Signature Creation Device

PKCS#11 Public Key Cryptography Standards

OID Object Identifier, en français identifiant d'objet.

Index

S