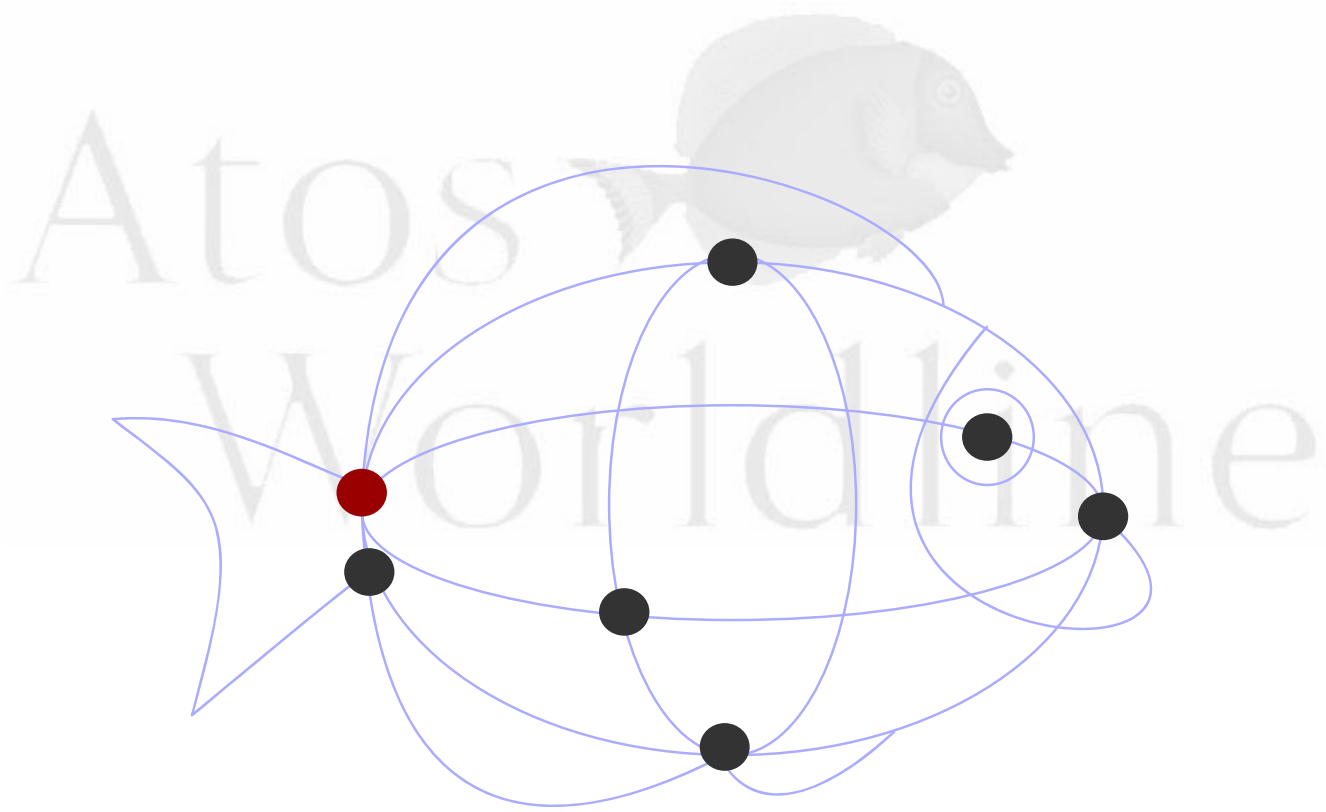
Référence du document :	WLS.AUD.0001
Révision du document :	6.0
Date du document :	27/05/2011
Etat du document :	BPA

Cible de Sécurité - Outil de signature Worldline Signer One



www.atosworldline.com

Table des matières

Historique des révisions de document

Version	Date	Auteur	Motif
1.0	27/01/2010	Atos Worldline	Première version publique du document
2.0	11/08/2010	Atos Worldline	Prise en compte remarques internes, Prise en compte des évolutions fonctionnelles et IHM
3.0	01/10/2010	Atos Worldline	Prise en compte évolutions fonctionnelles et IHM
4.0	06/12/2010	Atos Worldline	Evolutions mineures, prise en compte commentaires
5.0	24/03/2011	Atos Worldline	Prise en compte version 1.7 du profil de protection
6.0	27/05/2011	Atos Worldline	Mise à jour de version de TOE

Tables des figures

1 Introduction.

1.1 Identification.

Ce document constitue la cible de sécurité de Worldline Signer One « Module de création de signature».

Elements	Valeur
Titre	**Cible de Sécurité - Outil de signature Worldline Signer One**
Référence document	**WLS.AUD.0001**
Auteurs	**Atos Worldline**
Version CC	**V3.1 Révision 3**
Référence TOE	**Worldline Signer One-1.1.2**
Numéro de Version ST	**6.0**
Mots clé	**Signature électronique, Application de signature électronique, Application de création de signature électronique, Applet**

1.2 Présentation générale de la cible d'évaluation (TOE).

1.2.1 Type de TOE.

La TOE est une application de création de signature électronique de documents destinée à des utilisateurs humains. Elle permet à ces utilisateurs d'appliquer une signature électronique à des documents qu'ils gèrent via leur poste de travail personnel

Cette TOE est conforme aux exigences du profil de protection ACSE [PP-01].

La TOE est constituée d'un module de signature électronique au format XAdES (mode détaché version 1.3.2), packagé sous forme d'une Applet Java et d'une DLL (Dynamic Load Library) Windows. Ce module s'exécute dans un navigateur Internet (en dehors du périmètre de la cible d'évaluation) ou au sein d'une application client (en dehors du périmètre de la cible d'évaluation).

1.2.2 Contexte de la TOE

L'outil de création de signature s'inscrit dans une démarche globale d'Atos Worldline qui vise à mettre en œuvre des processus complets de dématérialisation pour le compte de ses clients.

Ainsi en tant que prestataire de services de certification électronique conforme au RGS, Atos Worldline est à même d'opérer des infrastructures de gestion de clés produisant des certificats de signature délivrés avec un haut niveau de sécurité (RGS ***).

Par ailleurs, l'outil de création de signature d'Atos Worldline, lorsque qualifié au niveau standard, respectera les exigences du RGS des trois niveaux de sécurité (*, **, ***).
Dès lors, les procédés de signature électronique reposant sur l'emploi de cet outil, d'un SSCD, ainsi que de certificats de signature *** atteignent le niveau *** du RGS (décrit dans le document [RGS-A-3]) et peuvent bénéficier à ce titre de la présomption de fiabilité au sens du décret n° 2001-272."

1.2.3 Structure de la cible de sécurité.

Le présent document est construit selon un plan identique au profil de protection ACSE [PP-01], il en reprend les principaux points.

Le présent document est conforme aux exigences de la classe d'évaluation « ASE » du document [CC3].

Les chapitres

- *4 : Définition du problème de sécurité, (à l'exception du paragraphe 4.6)*
- *5 : Objectifs de sécurité*
- *6. : Exigences de sécurité*

Sont strictement repris du profil de protection [PP-01]

Le chapitre

- *7 : Spécifications globales de la cible d'évaluation*

Est destiné à apporter des compléments sur la mise en œuvre du profil [PP-01] par la TOE.

1.2.4 Utilisation de la TOE.

La cible d'évaluation est le module Worldline Signer One permettant la création de signatures électroniques au format XAdES (mode détaché version 1.3.2), en s'appuyant sur un dispositif de création de signature externe (SCDev) (hors périmètre d'évaluation). Le module Worldline Signer One signe les documents au format :

- Texte.
- XML.
- PDF.
- Images (BMP).

Il fait partie d'un système global de création de signature électronique, incluant l'application et le dispositif de création de signature (SCDEV). Ce dernier est le seul à posséder la clé privée du signataire et à pouvoir l'utiliser pour des opérations cryptographiques. Il peut se présenter sous plusieurs formes, parmi lesquelles une carte à puce ou un token USB.

La TOE est exécutée suite à son appel par une "application" (nommée par la suite application appelante). Le ou les documents à signer sont passés à la TOE sous forme d'un paramètre. Plusieurs autres informations sont aussi transmises en paramètre pour préciser le déroulement de la signature (cf. §2.2.2).

La TOE est chargée sur le poste client. L'application appelante utilise le module en fonction de l'environnement dans lequel le module sera exécuté (type de machine et système d'exploitation).

L'application appelle ensuite le fichier du module Worldline Signer One qui saura être interprété correctement par l'environnement dans lequel il s'exécutera.

1.2.5 Environnement technique de la TOE.

Pour fonctionner, la TOE nécessite les éléments suivants :

- La plateforme hôte ;

- Les composants logiciels permettant de communiquer avec le dispositif de création de signature (SCDev) ;
- Un dispositif de création de signature électronique.

1.2.5.1 La plateforme hôte.

La plate-forme sur laquelle est exécutée la TOE est hors périmètre. Cette plate-forme comprend :

- La partie matérielle de la machine hôte ;
- Le système d'exploitation ;
- Les environnements d'exécution (runtime) nécessaires :
  - JAVA : JRE 1.5
  - Windows Mobile : Compact Framework Dotnet 3.0.5

La TOE est évaluée sur les configurations suivantes :

Ordinateur personnel (PC) :

Matériel :

CPU : Intel Pentium 4 2.8 GHz / RAM : 512 Mo / Disque dur : 80 Go

Lecteur de carte à puce requis

Configurations logicielles suivantes :

	Internet Explorer JRE 5	FireFox JRE 5
Windows XP SP3	Module Java.	Module Java.
Windows Seven	Module Java.	Module Java.
Ubuntu 10.04	-	Module Java.

PDA :

Matériel :

CPU : PXA270 520 MHz Mémoire Flash de 128 Mo, SDRAM de 128 Mo

Lecteur de carte à puce requis

Configurations logicielles suivantes :

	Internet Mobile
Windows Mobile 6.1	Module DLL

1.2.5.2 Le fournisseur de service cryptographique.

Le fournisseur de service cryptographique est le « middleware » permettant à la TOE (ou à d'autres applications souhaitant l'utiliser) de communiquer avec le dispositif de création de signature. Ce middleware est généralement fourni par le constructeur du dispositif de création de signature et se présente notamment sous la forme d'une librairie conforme au standard PKCS#11,

1.2.5.3 Le dispositif de création de signature.

Les dispositifs de création de signature supportés par la TOE sont ceux disposants d'un fournisseur de service cryptographique, sous forme d'une librairie PKCS#11, et supporté par la plateforme hôte..

L'utilisation de dispositifs de création de signature évalués conformes avec le profil de protection [SSCD] permettent de créer des signatures conformes au [RGS_A_3].

Note :

Les supports de certificats logiciels (magasin de certificats) ne sont pas pris en charge par la TOE

1.3 Définition 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.

1.3.1 Références.

1.3.1.1 Références normatives.

[CC1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 3.1, Revision 3, July 2009.
[CC2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements. Version 3.1, Revision 3, July 2009.
[CC3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements. Version 3.1, Revision 3, July 2009.
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology. Version 3.1, Revision 3, July 2009.
[QUA-STD]	Processus de qualification d'un produit de sécurité – Niveau standard. Version 1.2 (cf www.ssi.gouv.fr).
[PP-01]	Profil de protection : Application de création de signature électronique (PP-ACSE-CCv3.1 Version 1.7)
[PP-SSCD]	Protection Profile - Secure Signature-Creation Device type 2 (pp0005b version 1.04) et type 3 (pp0006b version 1.05)
[RGS_A_3]	Référentiel Général de Sécurité : Fonction de sécurité Signature électronique Version 2.3

1.3.1.2 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]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques. 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.
[TS 101 903]	XML Advanced Electronic Signatures
[PKCS#1]	PKCS #1 – RSA Cryptography Standard Version 2.1 RSA Laboratories

2 DESCRIPTION DE LA CIBLE D'EVALUATION.

2.1 Architecture.

La figure ci-dessous présente une vue schématique de la cible d'évaluation et de son architecture interne. Afin d'en faciliter la lecture, sont aussi représentés quelques éléments externes : le middleware de communication avec le SCDev et le SCDev lui-même.

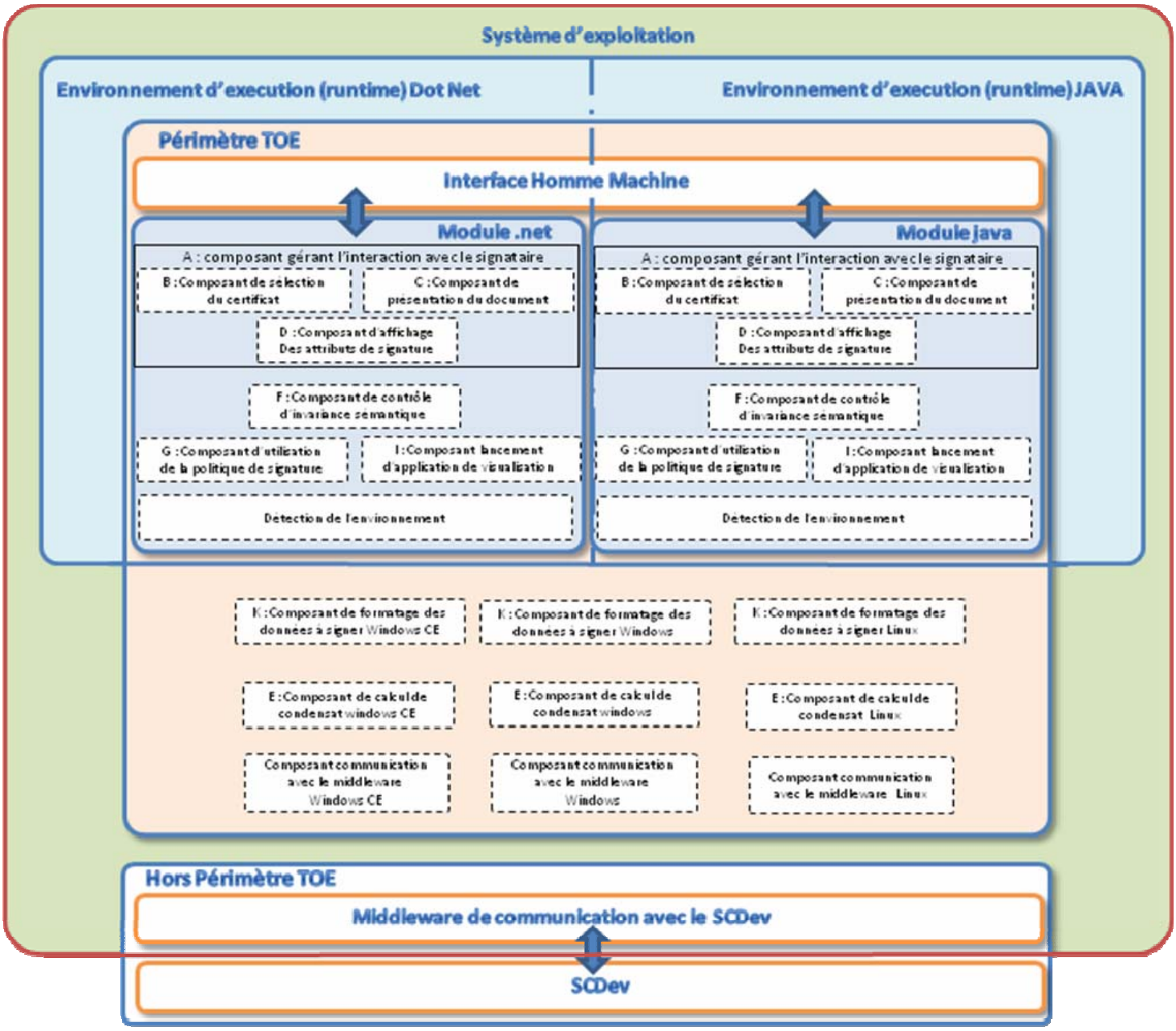


Figure 1 : Architecture Interne et interfaces de la TOE

En partant du haut vers le bas, nous distinguons sur ce schéma :

- L'appel à l'un des 2 fichiers suivant la plateforme cible ;
- Deux sous-ensembles représentant chacun des deux fichiers. Effectuant les mêmes opérations, ils sont découpés de manières identiques. Les composants les constituants sont décrits par la suite ;
- Le middleware de communication avec le SCDev, dépendant du couple système d'exploitation / navigateur ;
- Le dispositif de création de signature (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 une interface homme-machine permettant au signataire d'interagir directement avec la TOE,

Cette interface permet au signataire de :

- Sélectionner/désélectionner un ou plusieurs documents à signer.
- Visualiser ou renseigner 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 (module de communication SCDev).

2.1.1.1 Sélection/désélection des documents à signer.

La TOE supporte une IHM permettant au signataire d'indiquer le ou les documents qu'il souhaite signer.

Cette IHM permet à l'utilisateur signataire, de sélectionner/désélectionner un ou plusieurs documents à signer, il existe également la possibilité de sélectionner / désélectionner tous les documents à la fois (un seul clic).

Le contrôle de l'invariance sémantique ou le type de document à visualiser peuvent toutefois déterminer qu'un document n'est pas conforme à la politique de signature, la signature n'est alors pas autorisée par la TOE, même pour un document sélectionné

Document à signer et contre-signature.

La TOE ne prend pas en charge la contre signature.

Signature de un ou plusieurs documents.

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

2.1.1.2 Désélection de documents

Après avoir consulté un document sélectionné, le signataire peut refuser de le signer. La TOE permet ainsi de désélectionner un ou plusieurs documents déjà sélectionnés.

2.1.1.3 Sélection des attributs de signature

La TOE offre un moyen permettant au signataire de visualiser et/ou renseigner les attributs de signature à signer conjointement avec le document.

La politique de signature fixe les règles de gestion des attributs de signature

2.1.1.4 Composant de présentation de documents.

La TOE affiche le contenu du document à signer selon le format de celui ci.

La TOE vérifie systématiquement qu'elle est en mesure d'afficher le document (pas d'erreur de visualisation potentielle) avec les modules de visualisation dont elle dispose.

Si la TOE détermine qu'elle ne pourra pas afficher le document, la signature de celui-ci est refusée.

Note :

LA TOE n'appelle aucun module externe pour assurer la visualisation mais uniquement des modules de visualisation intégrés.

2.1.1.5 Composant de sélection du certificat.

Le composant de sélection de certificat récupère la liste des certificats présents dans le SCDev à travers le fournisseur d'accès aux services cryptographiques (cf. §1.2.5.2), puis présente à l'utilisateur la liste filtrée selon la politique de signature. L'utilisateur peut alors sélectionner son certificat.

Pour chaque certificat, les informations suivantes sont affichées :

- Le sujet certificat ;
- L'émetteur du certificat ;

Si un seul certificat est disponible à l'issue des contrôles et filtres. La TOE affiche directement ce certificat par défaut pour effectuer la signature.

2.1.1.6 Expression du consentement à signer

L'interface IHM TOE permet au signataire d'exprimer son consentement pour signer les documents.

Avant de lancer le processus de signature sur un ou plusieurs documents, la TOE identifie que le signataire souhaite signer.

Une interaction avec le signataire consiste à

- sélectionner le ou les documents qu'il souhaite signer.
- activer une boite à cocher indiquant explicitement son consentement

Ensuite le code pin d'activation du SCDev peut être saisi.

De plus, la TOE n'active pas le bouton « signer » sans cet enchainement d'action.

2.1.1.7 Contexte de signature

Il existe également un mode de fonctionnement (dit parapheur) de la TOE qui n'inclut pas la sélection préalable des documents à signer. Les documents sont alors présélectionnés par l'application appelante. La TOE permet toutefois d'accéder à la fonction sélection/désélection ainsi que la visualisation des documents dans ce mode.

La suite de l'expression du consentement reste identique.

Ce mode « parapheur » nécessite que l'application appelante respecte des exigences fonctionnelles fortes. Ces exigences sont précisées dans le guide de l'administrateur de sécurité, et s'imposent à lui pour activer le mode parapheur.

L'utilisation d'application appelante certifiée ou respectant les exigences RGS d'homologation du télé service, doit permettre de formaliser que ces exigences fonctionnelles sont respectées.

Le mode de fonctionnement de la TOE (standard ou parapheur) est un attribut de signature ; il sera donc inclus dans la signature du document. Il apparait également dans la fenêtre de signature (cf. 2.2.3 Exemple d'interface homme/Machine), avec la légende « contexte de signature » et peut prendre les valeurs :

- « None » (standard) (description du mode en 2.1.1.6)
- « parapheur » (description du mode en 2.1.1.7)

2.1.1.8 Interruption du processus de signature

La TOE permet au signataire d'interrompre à tout moment le processus de signature, c'est à dire jusqu'à l'action sur le bouton « signer » (correspondant à la transmission, par la TOE, des données à signer au SCDev).

Pour cela un bouton d'annulation est toujours disponible sur l'interface utilisateur.

2.1.2 Problématique du What You See Is What You Sign (WYSIWYS).

À l'instar du profil de protection [PP_01], cette problématique est traitée en trois parties :

- En permettant au signataire de visualiser le document à signer ;
- En participant au contrôle de l'invariance du document à signer, car contrairement aux documents papier, la sémantique des documents électroniques peut dans certains cas changer en fonction de l'environnement dans lequel ils sont visualisés. Nous parlons alors de contrôle d'invariance (ou de stabilité) sémantique ;
- Enfin, en permettant au signataire de visualiser les attributs qui seront signés conjointement avec le document.

Note :

La TOE ne s'appuie pas sur un module extérieur pour réaliser ces fonctions comme indiqué par le profil de protection **[PP-01]** (chapitre 5.1.6), car elle réalise elle-même l'ensemble de ces trois fonctions.

Le contrôle de l'invariance est donc réalisé systématiquement par un module intégré qui retourne les informations sur la stabilité sémantique du document.

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 permet, à la demande du signataire le lancement d'un module intégré de présentation correspondant au format du document à visualiser.

La TOE défini de manière statique, le module intégré de visualisation à utiliser, compte tenu du format de document concerné.

Note :

La TOE intègre des modules de visualisation intégrés à la TOE pour tous les formats de document suivants :

- XML, TXT, BMP. PDF

2.1.2.2 Composant de contrôle de l'invariance de la sémantique du document.

Un document à signer peut contenir des champs variables ou du code actif qui dépendent de paramètres extérieurs et qui pourraient, ainsi, être différents selon le contexte dans lequel le document est visualisé. Dans la suite du document, nous parlerons indifféremment d'invariance sémantique ou de stabilité sémantique.

La TOE permet de signer des documents

- Format « données brutes » (TXT, BMP),

Pour ces formats, les données brutes sont invariantes dans le temps par définition.

- XML

La TOE contrôle l'invariance de la sémantique du document en s'appuyant sur la définition des balises XML définies dans le guide d'intégration à l'intention de l'intégrateur, permettant d'interdire certaines balises qui introduirait une variance potentielle

- PDF

Pour un document PDF, l'invariance de la sémantique s'appuie sur le contrôle de la conformité avec la spécification PDF/A-1b (cf. [ISO 19005-1]).

L'invariance sémantique du document PDF est assurée par la conformité du document à la spécification PDF/A-1b. Cette spécification décrite dans la norme ISO 19005-1(cf. [ISO 19005-1]) assure la stabilité de la sémantique du document dans le temps.

Note :

Le contrôle de l'invariance est fait systématiquement par un module intégré à la TOE.

En cas de contrôle négatif la TOE ne permet pas de signer un document dont la stabilité sémantique n'est pas vérifiée.

2.1.2.3 Composant d'affichage des attributs de la signature.

Ce composant présente les attributs de signature au signataire.

Certains attributs de signature sont systématiquement présents dans la signature :

- La référence de la politique de signature.
- Le certificat de signature sélectionné par le signataire.
- Le contexte de signature (standard / parapheur)

D'autres attributs de signature (maximum 5) sont paramétrables au travers de la politique de signature, ils sont donnés ci-dessous à titre d'exemple.

- Le type d'engagement du signataire (si spécifié par la politique de signature).
- Le rôle du signataire (si spécifié par la politique de signature).
- La date de signature. Cette date est obtenue depuis la machine hôte. Elle constitue la date « présumée » de signature et ne doit pas être considérée comme un jeton d'horodatage.
- Le lieu de signature présumé (si spécifié par la politique de signature).

2.1.3 Composant d'utilisation de la politique de signature.

Ce composant applique tout au long du processus la politique de signature spécifiée par l'application appelante.

2.1.3.1 La politique de signature.

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

La TOE met en œuvre une politique de signature paramétrée par l'administrateur de sécurité l'administration de la politique de signature est réalisé en dehors de la TOE, cette politique est donc statique au sein de la TOE

La politique de signature comprend notamment les informations suivantes :

La politique contient les règles, portant notamment :

- sur les documents à signer (format) pouvant être signés par l'outil : quel type de document (pdf, txt, etc.) peut être signé.
- sur la signature (attributs de signature – liste et valorisation-, format de signature, algorithme de hachage, nombre de signature possible par authentification) :
  - quels sont les attributs de signature qui doivent être inclus dans la signature, et quelles valeurs possibles peut on y trouver,
  - quels algorithmes cryptographiques sont utilisés pour la signature,
  - combien de signatures peut-on appliquer lors d'une session ouverte avec le SCDev (après saisie du code d'activation, et avant une nouvelle saisie de ce code),
  - dans cette version de TOE, la seule possibilité de format de signature est *XAdES*
- sur les certificats applicables (filtres) : quel sont les certificats présents sur un SCDev, éligibles pour être proposé au signataire.

La politique de signature est protégée en intégrité par une signature électronique apposée par l'administrateur de sécurité et pouvant être identifié par son certificat. La vérification de la signature de l'administrateur de sécurité est réalisée par la TOE.

2.1.4 Composant de calcul de condensat

Ce composant formate le document à signer ainsi que les attributs de la signature puis les hache pour produire une information dénommée « condensé des données à signer formatées » qui sera envoyée au SCDev.

Note :

La TOE produit dans cette version des condensés selon l'algorithme SHA256

2.1.5 Composant de communication avec le middleware

Ce composant se matérialise sous la forme d'une librairie d'interfaçage au standard PKCS#11, il est mis à disposition généralement par le fournisseur du SCDev.

Ce composant permet de communiquer avec le « middleware de communication avec le SCDev ». Il est divisé en plusieurs sous-composants, en fonction de l'environnement dans lequel la TOE est exécutée.

Le composant de communication avec le middleware assure les fonctions suivantes :

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

La politique de signature peut indiquer que la session est ouverte sur le SCDev pour plusieurs signatures, ce fonctionnement n'est utilisable que dans le cas de signature de plusieurs documents et sous conditions que le module de communication avec le SCDev permette cette facilité.

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.

Note :

Mise en cache du code d'activation de la signature sur le SCDev :

Une information de la politique de signature indique le nombre maximum de signatures qui peuvent être enchainées, cela correspond donc également au nombre maximum de document que la TOE accepte pour un appel.

Si la TOE reçoit un nombre de documents supérieur au nombre maximum indiqué dans la politique de signature, le processus de signature redemande un pin code lorsque le nombre maximum est atteint

La TOE peut être amenée, si le SSCD et le middleware le permettent à conserver le code d'activation en mémoire pendant le nombre de signatures indiqué ci-dessus. Dans ce cas le code est protégé en mémoire.

2.1.6 Composant de formatage des données à signer.

Ce composant construit la structure de signature électronique au format XML XAdES version 1.3.2.

La TOE crée des signatures détachées.

Le niveau XADES produit est la forme XADES EPES simple, et ne contient donc pas de jeton d'horodatage.

2.1.6.1 Le format XAdES.

La syntaxe XML et les règles de traitement pour créer et représenter des signatures digitales sont données par le standard DSig (Digital Signature). Les signatures XML peuvent s'appliquer sur n'importe quel contenu digital objet de données, y compris un code XML.

Les spécifications XAdES (ou Xml Advanced Electronic Signature) prolongent celles de DSig dans le domaine de la non-répudiation en définissant des formats pour les signatures électroniques qui doivent restées valides pendant de grandes périodes et être conformes à la "Directive 1999/93/EC du parlement Européen et du conseil du 13 décembre 1999 sur le cadre communautaire des signatures électroniques".

Les éléments ajoutés par XAdES EPES au format XML-DSig sont principalement

- les attributs de signature,
- les données de validation
- La référence à une politique de signature

2.1.7 Composant de détection d'environnement.

La TOE effectue elle-même une détection d'environnement afin de déterminer à quel sous-composant de communication avec le middleware du SCDev elle devra faire appel.

2.2 Environnent d'utilisation de la TOE

2.2.1 Représentation physique.

La TOE est composée de deux types de livrables : correspondant à des environnements d'exécution différents, ils effectuent cependant les mêmes opérations :

- Un exécutable (exe) et une DLL qui s'exécutent en environnement Windows Mobile 6.1. il s'agit de code développé pour le framework .net dans sa version spécifique pour terminaux mobiles (autrement appelé Compact Framework) en version 3.5.
- Une applet Java dédiée à la JVM Sun (fichier jar) s'exécute sous de nombreux types de systèmes d'exploitation et navigateurs (cf. §1.2.5), à condition que la JVM Sun soit installée sur la machine hôte. La version de l'évaluation est la JVM 1.5.

Dans les 2 cas le code est fourni signé afin d'en garantir l'origine et l'intégrité.

Ces 2 types de livrables utilisent tous un ensemble de DLL communes (compilées selon l'OS cible), ces DLLs prennent en charge

- Les fonctions cryptographiques mises en œuvre par la TOE
- Le formatage XADES utilisé pour la signature résultat

Les plateformes (hors périmètre), sur lesquelles est évalué le produit, sont définies au paragraphe 1.2.5.

2.2.2 Séquence d'exécution du module.

2.2.2.1 Principe

Le schéma ci-dessous permet de représenter les interactions entre les différents acteurs du processus de signature

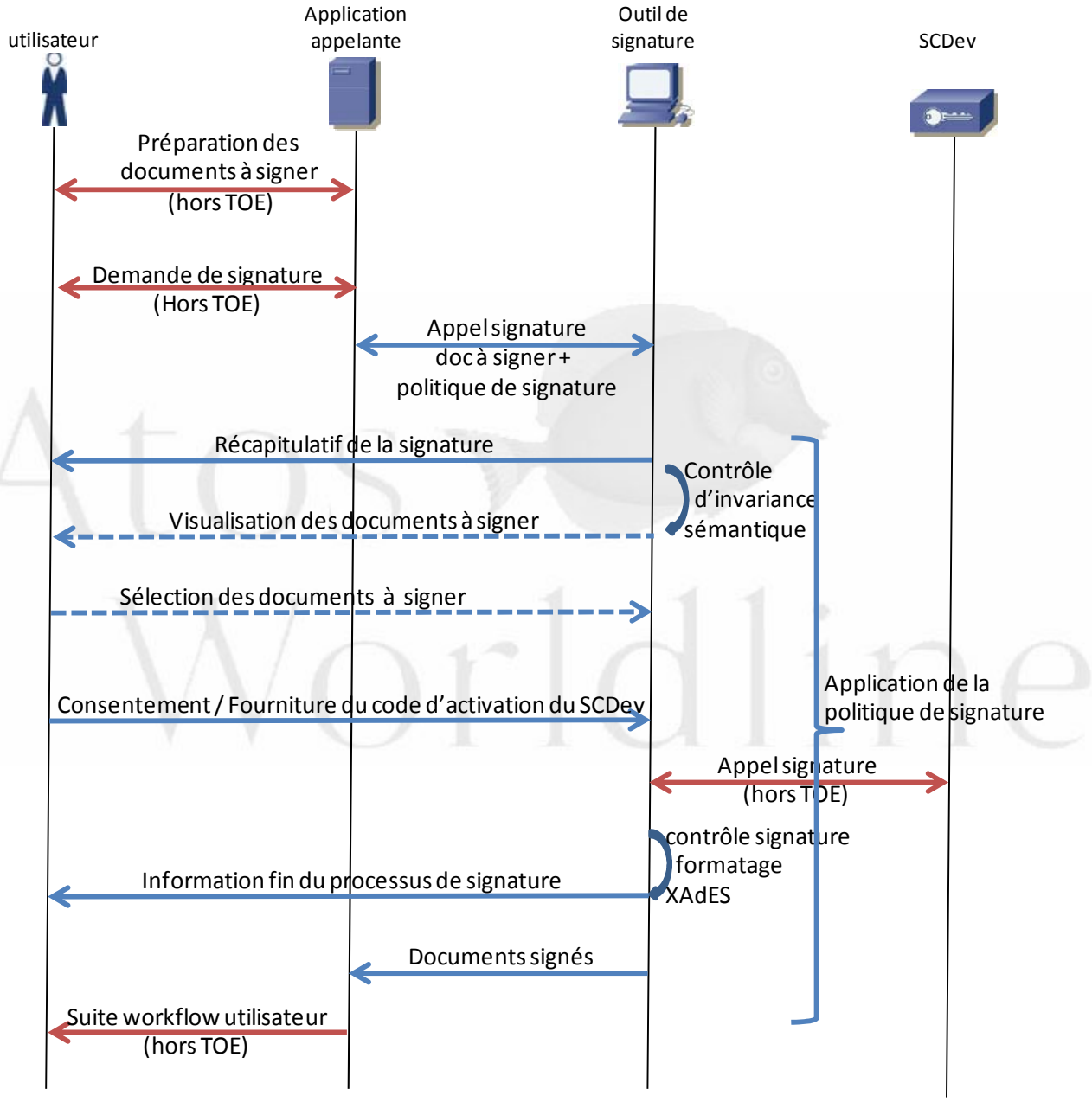


Figure 2 : Diagramme des échanges avec l'outil de signature.

2.2.2.2 Description

Les opérations effectuées par le module respectent la cinématique suivante :

- Le module Worldline Signer One est appelé par l'application appelante, avec en paramètres :
  - Le document ou les documents à signer, sous forme de la référence absolue du document.
  - Un scellement de la liste des documents
  - La référence de la politique de signature à appliquer (cf. paragraphe 2.1.3.1).
  - La page web vers laquelle le signataire sera dirigé une fois sa signature créée.
  - La page web en cas d'échec ou d'annulation de la signature.
  - La version de la signature XAdES à générer et le format. Les versions disponibles sont : 1.3.2
- Le module contrôle l'intégrité de la liste des documents et le contenu et l'intégrité du ou des document(s)
- Il affiche ensuite à l'utilisateur :

✓ La page de sélection des documents à signer

- En mode standard : la liste des documents reçus avec leur statuts, les options graphiques de sélection / désélection / visualisation des documents, un compteur de documents sélectionnées sur le nombre de documents total.
- En mode parapheur cette fenêtre est accessible via un bouton de visualisation de la liste des documents

✓ La page principale de l'application : accessible à partir de la précédente en mode standard ou directement en mode parapheur :

- Un compteur des documents reçus, (par la TOE et sélectionnés par l'utilisateur pour signature)
- Un bouton action permettant d'accéder à la liste des documents, et les visualiser
- Les attributs de signature requis par la politique de signature (cf. paragraphe 2.1.1.3)
- La description textuelle de la politique de signature appliquée.

  Le ou les certificats répondant aux contraintes introduites par la politique de signature.
- Il présente, sur demande du signataire, le détail du certificat de signature à utiliser
- Une boite à cocher permettant l'expression du consentement

- La partie inférieure de l'IHM permet la saisie du code d'activation du SCDev pour accéder à la clé de signature. Cette fenêtre comprend
  - Un champ de saisie du code d'activation,
  - Le bouton de déclenchement de la signature,
  - Le bouton d'annulation du processus de signature.

- Après saisie du code d'activation et validation explicite du signataire (bouton « signer »), la TOE :
  - Calcule le condensat des données à signer formatées.
  - Puis envoie au dispositif de création de signature le condensat, accompagné de la référence de la clé privée à utiliser (alias).
- Le dispositif renvoie le chiffré du condensat (Format PKCS#1).

- La TOE effectue une vérification cryptographique de la signature reçue par rapport au certificat que le signataire a choisi.
- Si la vérification est positive, la TOE formate ensuite une signature XAdES et renvoie l'ensemble à l'application appelante.
- La TOE présente au signataire la liste des documents qui ont été signés

2.2.3 Exemple d'interface homme/Machine

Les représentations d'écran schématiques ci-dessous ont pour but de donner une première appréciation du résultat final de la TOE en terme d'interaction avec l'utilisateur, et notamment la mise en œuvre d'un certain nombre de principes de fonctionnement.

2.2.3.1 Ecran d'accueil

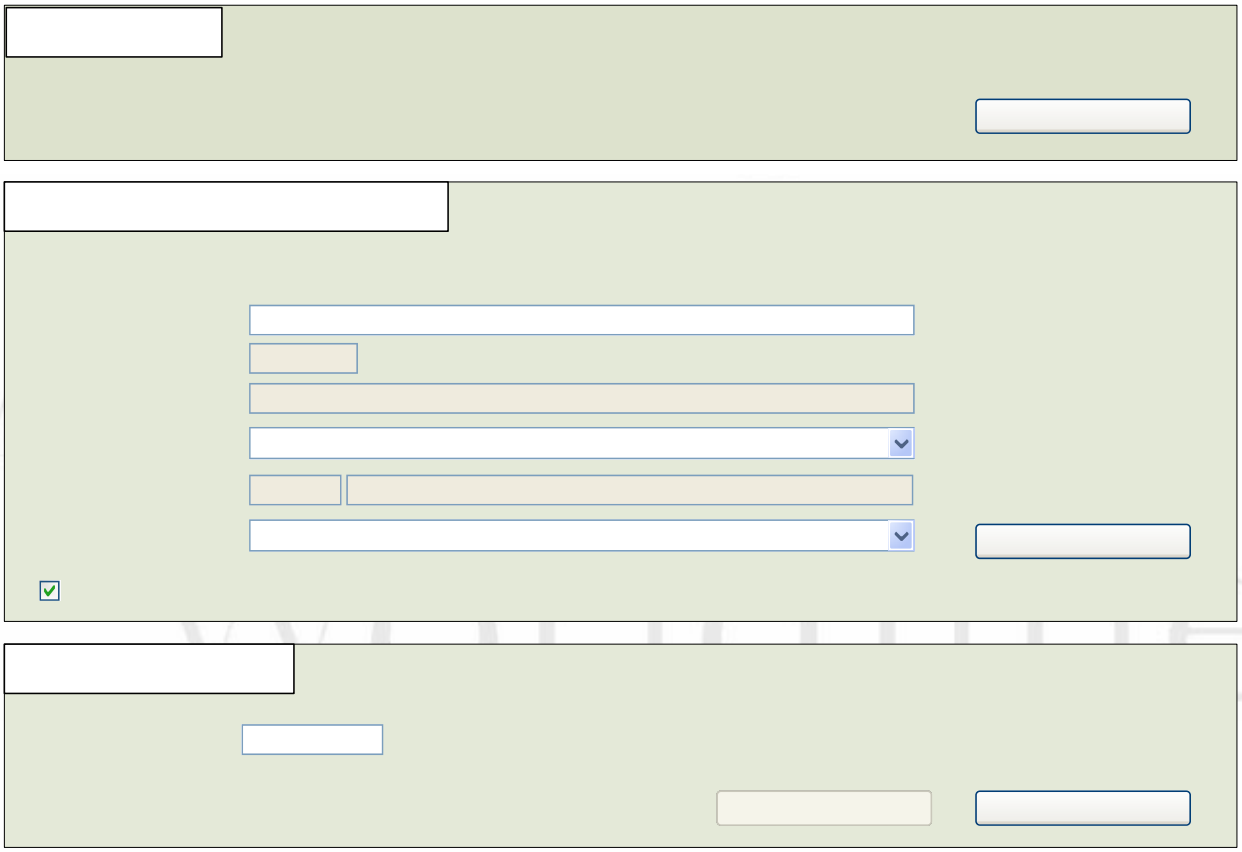


Figure 3 : exemple de page principale d'application.

Cas particulier :

Dans le cas où la TOE ne dispose que d'un seul certificat utilisable conformément à la politique de signature, il est sélectionné par défaut

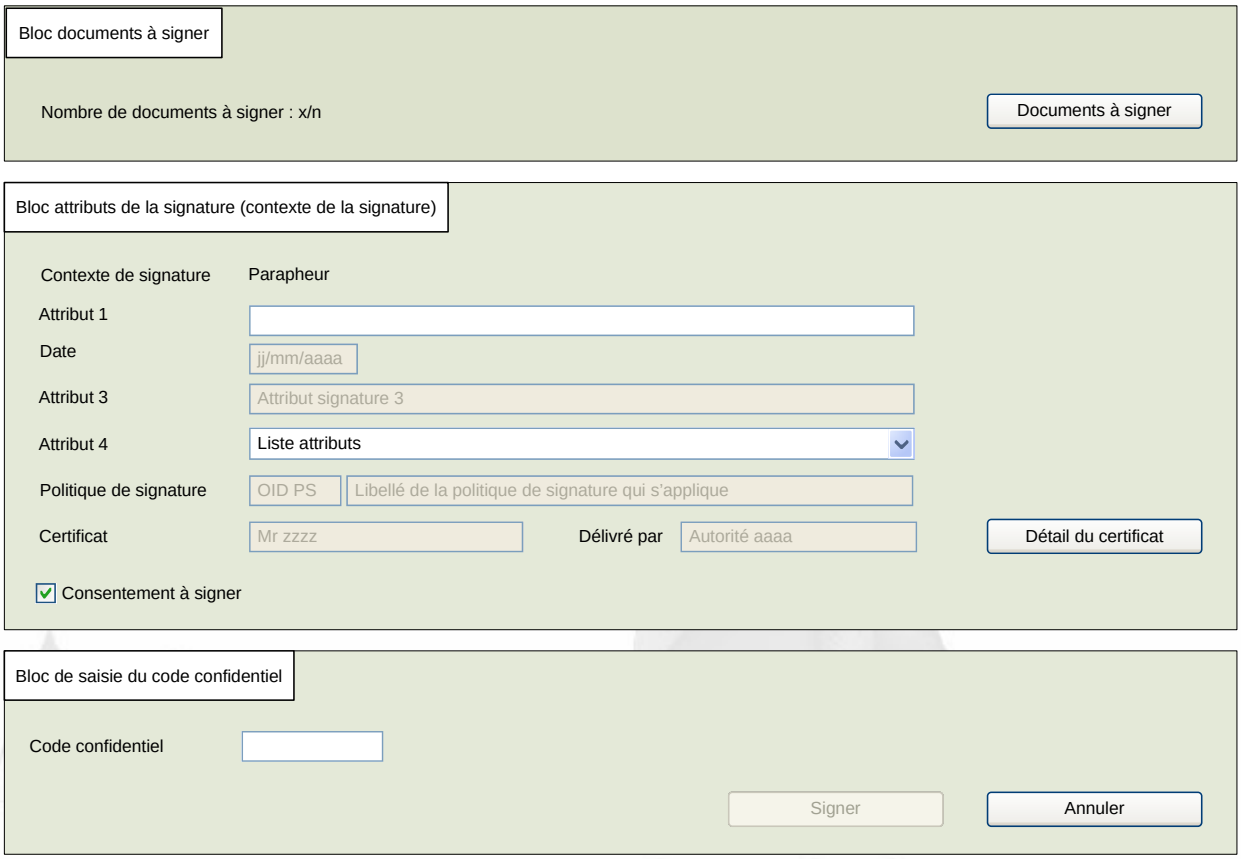


Figure 4 : exemple d'écran d'accueil avec certificat unique.

2.2.3.2 Ecran après consentement de signature

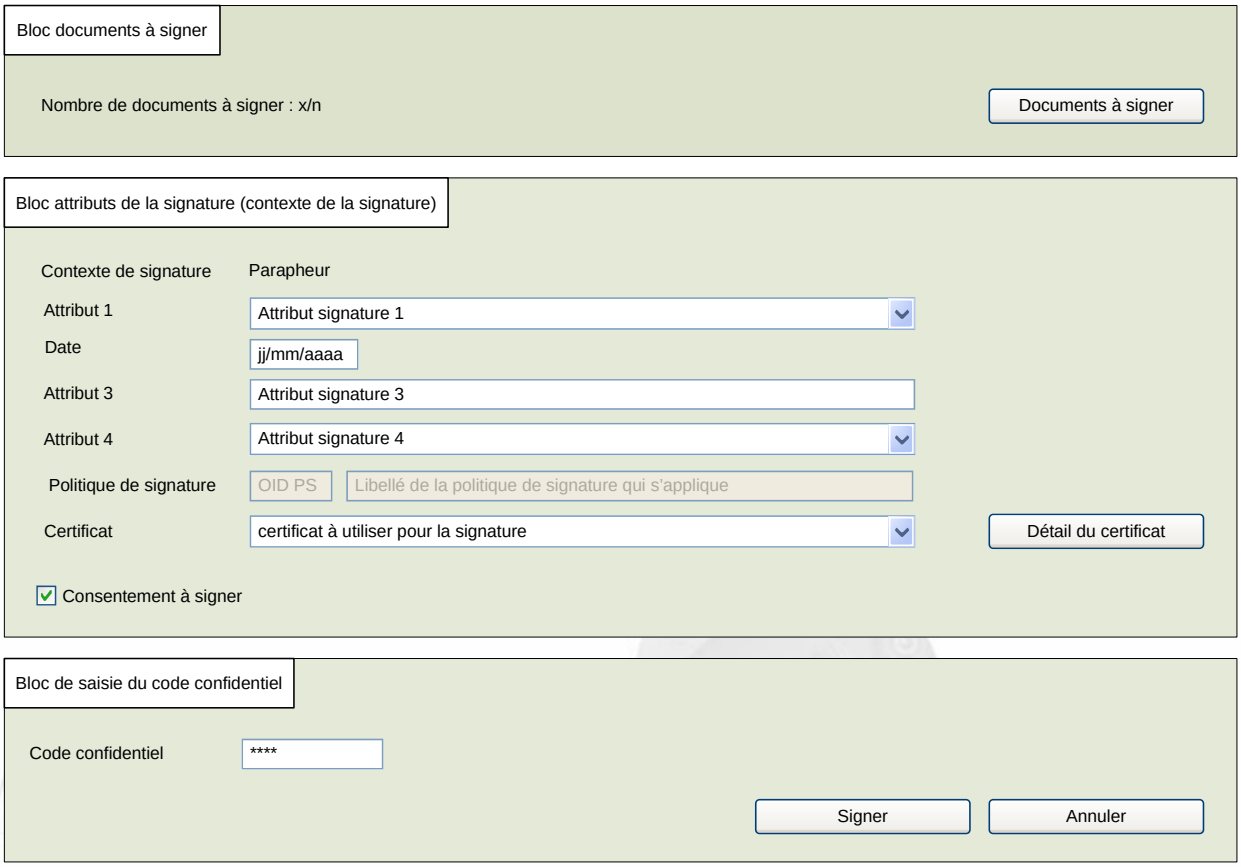


Figure 5 : exemple d'écran après consentement à signer.

2.2.4 Liste des documents à signer

- En mode standard, cette fenêtre est affichée automatiquement lors de l'appel de la TOE elle peut ensuite être ré-accédée par le bouton action « **documents à signer** »
- En mode « parapheur » cette fenêtre est accessible par le bouton action « **documents à signer** », tous les documents sont présélectionnés par avance.

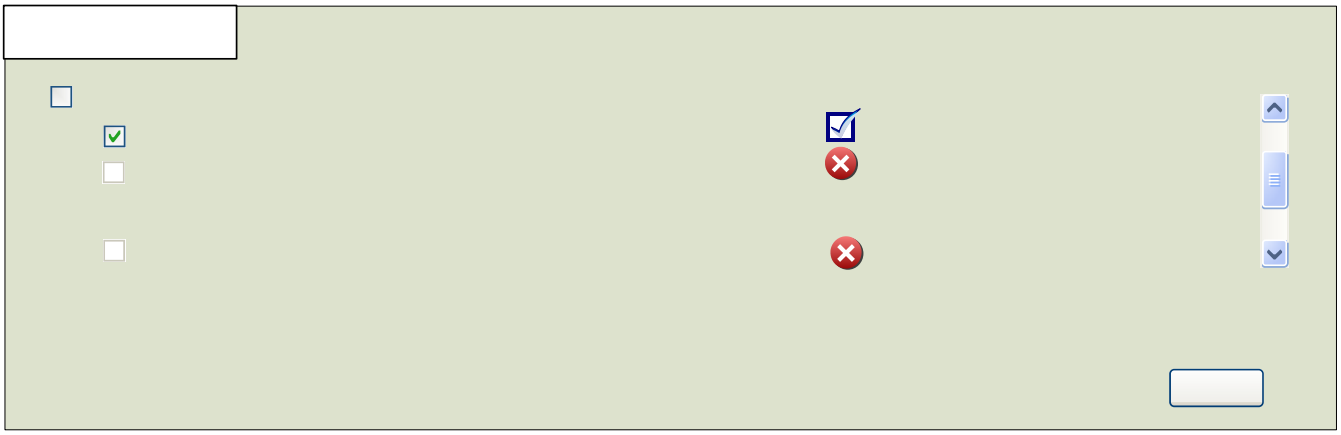


Figure 6 : liste des documents à signer

2.2.5 Détail du certificat

Cette fenêtre est affichée lorsque l'utilisateur sélectionne le bouton « ***Détail du certificat*** » dans l'exemple de la Figure 5

Figure 7 : détail du certificat

2.2.6 Ecran résultat de signature (optionnel)

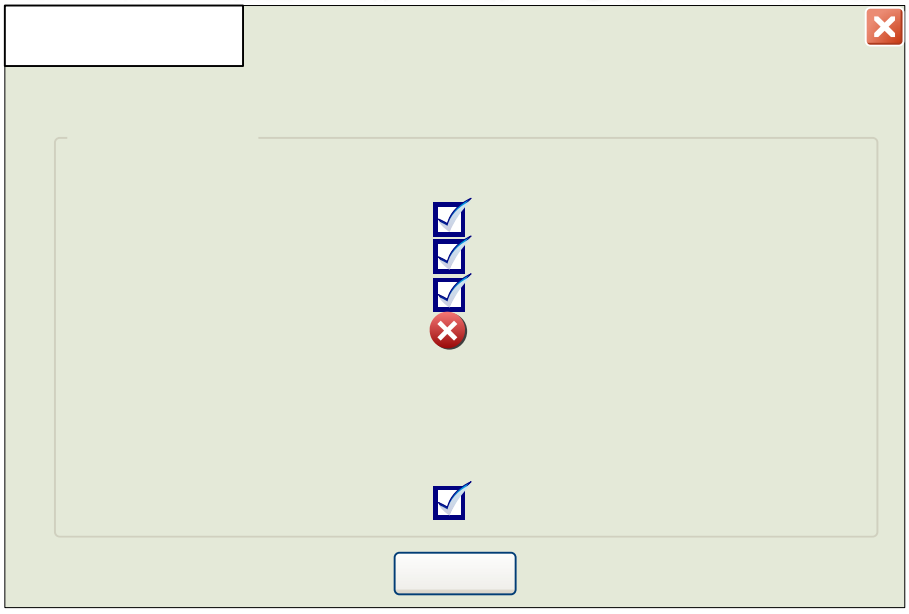


Figure 8 : écran résultat de signature

3 Déclaration de Conformité.

3.1 Déclaration de Conformité aux CC.

Cette cible de sécurité est strictement conforme aux Critères Communs version 3.1 Rev.3. Le document a été écrit conformément aux :

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

3.2 Déclaration de conformité à un Paquet.

Le niveau de conformité de la cible de sécurité est EAL 3+.

Le tableau ci-dessous indique quels sont les composants d'assurance du paquet EAL 3

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

Figure 9 : composant d'assurance EAL 3

Le niveau des exigences d'assurance de sécurité EAL 3 est augmenté par les composants

- AVA_VAN.3 Focused vulnerability analysis
- ALC_FLR.3 Systematic flaw remediation.

Note : Ce niveau d'assurance correspond aux paquets d'exigences définies par l'ANSSI pour le niveau de qualification au niveau standard. [QUA_STD].Conformité à un PP.

3.3 Conformité à un PP.

La Cible de sécurité du produit Worldline Signer One, « Module de création de signature » est strictement conforme au profil de protection « Application de création de signature » [PP-01].

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 :

- Un unique document électronique.
- Plusieurs documents électroniques.

Protection : intégrité, confidentialité

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 (OID) 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.
- Le rôle du signataire.

Protection : intégrité, confidentialité.

B.Données_A_Signer_Formatées.

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

Note :

Message XML conforme à la norme XADES (SignedInfo, SignedProperties).

Protection : intégrité, confidentialité.

B.Condensé_Des_Données_A_Signer.

Cette donnée est un condensé des données à signer formatées (selon le standard XADES).

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.

Note :

Ces informations sont détaillées dans la norme XADES.

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.

La modification non autorisée de la politique de signature est détectée et entraine un arrêt du processus.

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.

Note :

La correspondance est une donnée de la politique de signature.

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.

Note :

La correspondance est une information de la politique de signature.

Protection : intégrité.

4.2 Sujets.

S.Signataire.

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

Note :

Le signataire peut aussi interagir avec la TOE via une application appelante qui formate des requêtes de demande de signature et fait référence à une politique de signature, pour déterminer le contexte de la signature. L'application appelante reçoit la réponse à sa requête, contenant le résultat de la signature ou une notification d'erreur.

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.

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).

S.Application appellante .

L'application appelante ne fait pas partie de l'évaluation de la TOE, elle utilise la TOE et ne peut modifier aucun bien sensible hors de son périmètre.

Le document à signer est produit et / ou manipulé par l'application appelante avant sa communication à la TOE.

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 les deux points suivants :

- Que les attributs de signature sélectionnés par le signataire sont bien conformes à la politique de signature à appliquer.
- 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.

Si un document est déterminé comme non stable, la TOE en informe l'utilisateur et interdit le processus de signature de ce document.

4.4.3 Présentation du document et des attributs de signature au signataire.

P.Possibilité_De_Présenter_Le_Document.

La TOE permet au signataire d'accéder à une représentation fidèle du document à signer.

La TOE ne permet 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 sont 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.

D'autres informations facilitant la vérification de la signature peuvent être ajoutées (ex : le certificat du signataire in extenso, ,la date et lieu présumés de signature ainsi que des attributs de signature tels qu'ils sont définis par la politique de signature etc.).

P.Administration.

La TOE doit permettre à l'administrateur de sécurité de gérer (ajouter/modifier/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.

Le rôle d'administrateur de la machine hôte mentionné ci-dessus est différent 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.

Note :

Du fait que la machine hôte est sous le contrôle de l'administrateur (mentionné ci-dessus), la date et l'heure de la machine sont considérées comme correctement réglées et leurs changements non accessible à l'utilisateur.

4.5.1.2 Hypothèses relatives au 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].

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.

Les composants assurant la communication entre la TOE et le SCDev sont composés de différents composants logiciels et/ou matériels installés sur le système d'exploitation du poste du signataire (ex : les pilotes PKCS#11 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 retranscrivent fidèlement le type du document à signer.

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.

[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.

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.

5 Objectifs de sécurité.

Pour certains objectifs il est précisé dans une note d'application quels sont les points qui ne sont pas retenus ainsi que la raison de cette suppression.

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 :

La référence de temps quand elle est utilisée, 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.

:

D'autres informations facilitant la vérification de la signature sont ajoutées (ex : le certificat du signataire in extenso, la date et lieu présumé de signature ainsi que des attributs de signature tels qu'ils sont définis par la politique de signature etc.).

5.1.4 Protection des données.

O.Administration

La TOE devra permettre à l'administrateur de sécurité de gérer (ajouter/modifier/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 informe 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 interdira la signature du document jugé non stable

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 permet 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 est 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.

La machine hôte peut également utiliser un seul contexte d'exécution une seule tache (Windows mobile)

Les mesures suivantes devront être appliquées :

- La machine hôte est protégée contre les virus quand de telles protections existent.
- 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 ou utilisent des réseaux privés sous le contrôle de l'organisation à laquelle le signataire appartient.
- 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.

Le rôle d'administrateur de la machine hôte mentionné ci-dessus est différent 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.

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.

Note :

La TOE assure elle-même la visualisation du document à signer.

5.2.5 Divers.

OE.Contrôle_Sémantique_Document_à_Signer.

L'environnement de la TOE devra fournir une fonction capable de déterminer si la sémantique du document à signer est bien invariante et de communiquer le statut de son analyse à la TOE.

Note :

La TOE assure elle-même le contrôle de la sémantique du document à signer.

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 et l'administration 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.

Dans le texte qui suit, ces raffinements sont notés ainsi : [raffinement éditorial : texte du raffinement éditorial]

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.

Dans le texte qui suit ces raffinements sont notés ainsi : *raffinement* : texte du raffinement

Les affectations requises par le profil de protection [PP-01] sont notées ***[Affectation : texte de l'affectation],*** tandis que les affectations issues des critères communs [CC2] sont indiquées en gras dans le texte.

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 certificate 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
- 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
[*Affectation: following additional rules:*

- **The format of the document is known by the TOE,**
- **The format of the document is listed in the signature policy,**
- **The document integrity is successfully controlled,**
- **The total size of all documents to be signed is limited by the TOE, this size cannot be changed. (the limit is mentioned in the integration guide)**
- **The size of each document is limited by the TOE and specific for each format of document, these limits cannot be changed (these limits are mentioned in the integration guide for each formats)**
- **The TOE shall not accept more than 100 documents to be signed]**

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

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

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

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

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

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

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

FDP_ITC.1.3/Document acceptance The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE:

- **determine whether the document's semantics is invariant or not by invoking a dedicated external module,**
- **the document shall invoke 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.

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.

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:

[Affectation:

- **Signer's certificate is signed by a certificate Authority referenced by the signature policy**
- **the certificate must belong to the certificates range, if mentioned by the SFP]**

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 the
[Affectation:
following rules : Signer certificate must be an X509 certificate, compliant with the RFC 5280

- **Signer's certificate must be successfully parsed regarding to these standards**
- **Resulting to this parsing the TOE will retrieve**
  - **The subject (Distinguish Name).**
  - **The serial number.**
  - **The issuer (DN of Certificate Authority).**
  - **OID (Object Identifier).**
  - **The validity dates (Not Before, Not After).**
  - **The Key usage.**

- **QC statements (if applicable)]**

when interpreting the TSF data from another trusted IT product :

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, *[Affectation* : no other attribute]), signer's explicit agreement to sign the present non invariant document (see *FDP_IFF.1.2/Signature generation*, the SCDev (*[Affectation: no SCDev 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, list of supported signature attributes**:

[*Affectation:*

- ***application specific signature attributes under specific rules, the list of these signature attributes is defined in the signature policy and describe for each attribute:***
  - ***an attribute's name,***
  - ***a text to be displayed (caption of the attribute) to the signer on the main signature screen,***
  - ***several parameters defined to apply specific rules(cf. FDP_IFF1.2/signature generation simple security attribute).***
    - ***default value***
    - ***list of allowed values***
    - ***optional or not***
    - ***modifiable or not***
- ***the TOE does not accept more than five 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;**

[Affectation:

If the signature policy set up additional signature attributes; then these rules must be applied:

- **the signature attribute must be uniquely named**
- **The signature attribute must be defined as optional or required (no default choice)**
- **The signature attribute may have a default value**
- **The signature attribute may be filled either by the signer or the calling application**
- **The policy must defined if the signer may change the signature attribute value or not**
- **The signature policy may define a list of valid values for the signature attribute**

The TOE cannot accept more than five security 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 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:

[Affectation:

- **The signer must select one or several documents to be signed**
- **The signer must type the activation code for the SCDev to confirm its agreement]**

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 ([Affectation: No additional security attribute])**
  - **the SCDev (the status of signature generation process,[Affectation: No other SCDev attribute])**
- **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, [Affectation: no additional signature attribute].**

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:
[Affectation: *No additional 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
[Affectation: SHA-256] and cryptographic key sizes
[Affectation: fingerprint length: 256 bits] that meet the following ***CRYPT-STD***,
[Affectation: FIPS Pubs 180-3].

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 [Affectation: no function for] the document format/viewer association table.**

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 ***[Affectation: no allowed management operations]*** the **signature policies** to **the security administrator of the TOE**.

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: ***[Affectation: no management functions provided.]***

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.

Note

Les composants prévus par le paquet d'assurance EAL de niveau 3 augmenté, sont ceux listés dans le paragraphe 3.2 Déclaration de conformité à un Paquet.

7 SPECIFICATIONS GLOBALES DE LA CIBLE D'EVALUATION.

7.1 Fonctions de sécurité

7.1.1 Utilisation de la politique de signature

Cette fonction permet de piloter le comportement de la TOE tel que l'a déterminé l'administrateur de sécurité. L'application appelante ou le signataire ne pourront intervenir dans la TOE que dans le cadre restrictif décrit par la politique de signature.

Cette fonction offre les services suivants :

- Vérifier la conformité de la politique de signature (validité dans le temps, authentification de l'émetteur de la politique, intégrité de la politique, conformité sémantique). A l'issu de cette vérification les informations données par la politique à la TOE son réputées fiables
- Donner les informations permettant de filtrer les certificats de signature autorisés (autorité émettrice, gamme de certificat)
- Donner les informations sur les attributs de signature à inclure ainsi que une possible valorisation automatique ou un mode de saisie par le signataire.
- Lister les formats de documents autorisés pour signature par la TOE, ainsi que les modules de visualisation à utiliser pour chacun des formats listés
- Indiquer l'algorithme de signature à mettre en œuvre
- Indiquer le format de signature final en réponse par la TOE
- Condition de signature : limite le nombre de signatures autorisées lors de l'appel de l'outil.

7.1.2 Contrôler les documents à signer

La TOE analyse la liste des documents transmise par l'application appelante :

- Contrôle d'intégrité : la liste de document reçue par la TOE correspond à celle transmise par l'application appelante.

La TOE analyse chaque document que l'application appelante lui transmet et ne permet pas la signature d'un document dont un contrôle préalable n'a pas été effectué.

- Contrôle de format : le document a un format autorisé par la politique de signature
- Contrôle d'intégrité : le document reçu par la TOE correspond à celui transmis par l'application appelante
- le contrôle d'invariance : le document ne peut être altéré en fonction de l'outil de visualisation utilisé.

Si les contrôles ne sont pas tous positif pour un document, la TOE ne permet pas la signature de ce document.

7.1.3 Gestion des documents à signer

- La TOE contrôle la stabilité sémantique de chaque document à signer que lui fournit l'application appelante en utilisant ses propres modules intégrés de validation.
- La TOE donne accès à la liste du ou des documents à signer, les documents non stables apparaissent dans cette liste mais ne sont pas sélectionnables.
- la TOE permet au signataire de sélectionner parmi ces documents celui ou ceux qu'il veut signer,
    - o en mode standard,(par défaut), la TOE ne présélectionne aucun document. En contrepartie, elle permet de désélectionner un ou plusieurs documents qui auraient été préalablement sélectionnés.
    - o En mode parapheur, la TOE présélectionne les documents à signer, elle permet de désélectionner un ou plusieurs documents qui auraient été préalablement sélectionnés
- La TOE permet d'invoquer un module de visualisation intégré pour chaque format de document

7.1.4 Gestion des attributs de signature

La TOE présente, sous contrôle de la politique de signature, les attributs de signature, cette présentation est faite avant l'expression du consentement de signature

La TOE peut soit

- afficher les attributs déjà renseignés automatiquement,,
- soit demander au signataire de saisir la valeur des attributs.

Si un attribut en saisie, est déterminé obligatoire, l'expression du consentement ne pourra se faire tant que la saisie ne sera pas complétée en cohérence avec la politique de signature.

7.1.5 Sélection du certificat

La TOE fait appel au SCDev pour obtenir la liste des certificats présents.

La TOE utilise la politique de signature pour filtrer les certificats « éligibles » à la signature,

- Ces certificats doivent être émis par une AC autorisée.
- Si une gamme est spécifiée le certificat du signataire devra en faire partie
- Les Certificats sont effectivement émis par une AC citées dans la politique de signature
- les certificats sont valides en regard à la date système du poste hébergeant la TOE

La TOE présente à l'utilisateur le ou les certificats répondant aux contraintes de filtrage.

En complément du choix du certificat, le signataire peut demander de voir le contenu complet du certificat qu'il a choisi, ceci n'est pas obligatoire pour autoriser le consentement explicite du signataire pour déclencher la signature.

7.1.6 Gestion du consentement ou de l'abandon de signature

La TOE demande à l'utilisateur une série d'action sur l'IHM pour exprimer son consentement explicite :

- Sélection des documents qu'il souhaite signer (par défaut en mode parapheur les documents sont déjà sélectionnés)
- saisie du code d'activation du SCDev

A partir de ces deux actions complétées, la TOE active le Bouton action « Signer »

A tout moment la TOE propose le bouton « d'annulation » permettant d'interrompre le processus de signature

7.1.7 Fonctions cryptographiques

La TOE utilise plusieurs fonctions cryptographiques :

- Calcul de Hash, ce calcul est utilisé pour préparer la signature par le SCDev, il est intégré à la TOE
- Vérification de signature RSA avec une clé publique. Cette fonction est utilisée
  - pour valider la politique de signature produite et signée par un administrateur,
  - pour vérifier la signature d'un certificat du signataire par son AC émettrice (chaine de confiance)
  - pour vérifier le retour de signature du SCDev

7.1.8 Interaction avec le SCDev

La TOE fait appel au SCDev pour plusieurs services :

- Fournir la liste complète des certificats stockés dans le SCDev
- Authentifier le signataire au moyen de son code PIN
- Etablir un canal de communication avec le SCDev
- Obtenir du SCDev une signature en utilisant une clé privée stockée

7.1.9 Formatage de la signature finale

La TOE collecte les informations nécessaires au formatage de la signature dans le format spécifié par la politique de signature

Le formatage consiste alors à coder une signature conforme au standard XADES incluant l'ensemble des données requises

- La signature numérique du document
- Le condensé de l'ensemble des données à signer (le document et les attributs de signature)

- Les attributs de signature
- Le certificat complet du signataire.
- Une référence à la politique de signature appliquée
- Une référence au document signé

7.1.10 Retour de la signature produite

La TOE produit à destination de l'application appelante plusieurs informations :

- L'ensemble des signatures de documents qui ont été contrôlés, approuvés par le signataire et signés
- Un Compte rendu d'exécution
- Un fichier log d'exécution (journal d'exécution)

7.2 Spécification globales par exigences de sécurité

FDP_IFC.1/Document acceptance	la stabilité du document est vérifiée à l'importation du document à signer. Si le document est jugé instable, le signataire en est informé et le processus est refusé pour ce document. La TOE contrôle le format du document lors de l'importation. Les formats listés dans la politique de signature sont seuls autorisés. La TOE contrôle l'intégrité de chacun des documents transmis par l'application appelante La TOE contrôle systématiquement tous les documents importés. La TOE fournit au signataire une mention d'invariance du document à signer. Le contournement de ces contrôles n'est pas permis par le TOE.
FDP_IFF.1/Document acceptance	
FDP_ITC.1/Document acceptance	Le contrôle de l'invariance du document à signer est réalisé par la TOE. Note : En l'absence d'outil de contrôle d'invariance sémantique qualifié, la TOE utilise son propre module intégré de contrôle.
FMT_MSA.3/Document's acceptance	Le comportement par défaut de la TOE lors de l'importation du document est géré par la politique de signature et n'est pas modifiable par le signataire. Seul l'administrateur de sécurité dispose des moyens de modifier le comportement de la TOE.
FMT_MSA.1/Selected documents	La liste des documents à signer est initialisée par l'application appelante. La TOE n'a pas de fonction lui permettant d'intervenir sur la liste pour la modifier.. La TOE contrôle l'intégrité de la liste des documents transmise par l'application appelante Le signataire peut désélectionner/sélectionner un document de la liste gérée par la TOE. La TOE ne permet pas de sélectionner un document instable. La TOE n'a pas de fonction de modification de la liste des documents à signer en ajout ou retrait.
FMT_SMF.1/Selection of a list of documents	
FMT_MSA.1/Document's semantic invariance	La stabilité d'un document à signer est déterminée par un module intégré à la TOE. Le comportement de ce module ne peut être modifié à aucun moment.
FMT_SMF.1/Getting document's semantics invariance status	Le contrôle d'invariance est effectué par un module intégré à la TOE
FMT_MSA.1/Signer agreement to sign	la TOE ne permet pas de signer un document instable En l'absence de module externe qualifiée pour déterminer le statut d'invariance d'un document, le statut est déterminé par un module intégré à la TOE
FMT_SMF.1/Getting signer	

agreement to sign	
FDP_ROL.2/Abort of the signature	L'interface homme /machine de la TOE propose toujours un bouton « annulation » à l'utilisateur lui permettant d'interrompre à tout moment le processus de signature, c'est-à-dire tant que le consentement de signature n'a pas été obtenu. La TOE retourne un statut d'abandon à l'application appelante
FMT_MSA.1/Signature attributes management	Les attributs de signature à ajouter sont fixés, par la politique de signature. Le signataire peut en choisir le contenu dans le cadre imposé par la politique de signature. L'attribut contenant le contexte de signature de la TOE (standard / parapheur) est obligatoire, il n'est pas modifiable par le signataire.
FMT_SMF.1/Modification of signature attributes	La politique de signature détermine pour chaque attribut les valeurs possibles que peut choisir le signataire, Si une seule valeur est possible, la TOE ne propose pas de choix au signataire mais prend la valeur indiquée. Le choix des valeurs d'attributs est laissé au signataire avant le déclenchement de la signature, il n'est plus modifiable à partir de là.
FDP_IFC.1/Signer's certificate	La TOE propose l'utilisation des certificats de signature (Key usage : non répudiation positionné) qui sont disponibles uniquement dans le SCDev La TOE filtre les certificats qui ne sont pas émis par une Autorité de Certification listée par la politique de signature. La TOE ne sélectionne pas les certificats qui ne sont pas émis dans une gamme de certificats (OID) listée par la politique de signature (ce paramètre est optionnel). Dans le cas où la politique détermine qu'un certificat de signature est qualifié (niveau RGS 3 étoiles), La TOE vérifie que les QC statements listés par le RGS sont présents dans le certificat. La TOE contrôle la signature du certificat par l'Autorité de Certification La TOE ne propose pas la signature avec un certificat n'ayant pas passé les contrôles et filtres indiqués ci-dessus
FDP_IFF.1/Signer's certificate	
FMT_MSA.3/Signer's certificate	La TOE indique les conditions de filtre applicables dans le choix des certificats adéquats pour signature. Ces conditions sont protégées par la TOE et ne sont pas modifiables par le signataire.
FMT_MSA.1/Signer's certificate	La TOE n'accepte pas d'informations sur le certificat à utiliser en dehors de la politique de signature. La TOE sélectionne les certificats présents sur le SCDev et demande au signataire de choisir celui qui servira à la signature.
FDP_ITC.2/Signer's certificate import	La TOE utilise le module de communication fourni avec le SCDev pour importer les certificats présents. La TOE utilise le certificat X509 qu'elle reçoit du SCDev. LA TOE contrôle la signature du certificat par l'autorité émettrice

FPT_TDC.1/Signer's certificate	La TOE utilise des certificats X509 conforme à la RFC 5280 ces certificats doivent être présents sur le SCDev utilisé pour la signature
FMT_SMF.1/Signer's certificate selection	La TOE utilise la politique de signature pour filtrer les certificats utilisables pour la signature. Le signataire choisit alors parmi les certificats respectant la politique de signature. Si un seul certificat est disponible la TOE affiche directement l'identifiant de celui-ci
FDP_IFC.1/Signature generation	La communication entre le signataire (via la TOE) et le SCDev, ne peut se faire qu'à l'intérieur d'une session authentifiée par un code d'identification numérique (PIN) saisi par le signataire. La TOE utilise le module de communication avec le SCDev pour ouvrir la session. La TOE veille à garantir l'intégrité des données lors de la phase de transfert entre la TOE et le SCDev, à savoir lors : • Du transfert du hash du document à signer ; • De la réception du hash signé (format PKCS#1). Pour ce faire, les contrôles suivants sont mis en œuvre : • Contrôler le hash (longueur) • Contrôler la signature (vérification de signature RSA)
FDP_IFF.1/Signature generation	Avant de donner accès à la signature la TOE : • Affiche les attributs de signature. • Affiche la liste des documents à signer, en présentant une mention de leur état d'intégrité et d'invariance. • Permet de visualiser le contenu du document (en sollicitant le module de visualisation correspondant au format du document) liste les certificats utilisables conformément à la politique de signature. La TOE communique la liste des attributs de signature conformément à la politique de signature. Les règles de valorisation de ces attributs sont fixées par la politique de signature. ✓ attributs obligatoires ou non, ✓ valeur libre (saisie manuelle) ou issue d'une liste ou valorisée par la TOE selon les critères de la politique de signature La TOE bloque le déroulement du processus de signature, si les

	attributs requis ne sont pas tous valorisés conformément aux règles mentionnées dans la politique de signature La TOE ne permet pas de signer un document dont le type n'est pas conforme à la politique de signature. La TOE ne permet pas de signer un document dont l'invariance sémantique n'est pas respectée.
FMT_MSA.3/Signature generation	Les valeurs par défaut des attributs de sécurité sont fixées dans la politique de signature. La TOE ou le signataire ne peuvent les modifier.
FDP_ITC.1/Explicit signer agreement	Dans l'interface homme-machine de la TOE : 1/ le signataire sélectionne les documents qu'il veut signer, par défaut les documents sont sélectionnés 2/Le signataire saisie le code d'activation du SCDev le bouton action « signer »devient alors actif. 3/ Le signataire peut alors cliquer sur le bouton de signature.
FDP_IFC.1/Electronic signature export	Le résultat de la signature est retourné à la TOE à l'intérieur de la même session authentifiée utilisée pour envoyer le hash du document à signer, et sélectionner la clé à utiliser. Le transfert des données du SCDev à la TOE s'effectue par le biais d'une opération unique (regroupement en un envoi de tous les documents signés).
FDP_IFF.1/Electronic signature export	La TOE utilise le retour du module de communication avec le SCDev pour déterminer si l'opération s'est bien déroulée. La TOE procède systématiquement à une vérification de la signature au niveau cryptographique en utilisant la clé publique présente dans le certificat sélectionné par le signataire.La TOE informe le signataire du résultat du traitement : réussite ou échec de la signature.
FDP_ETC.2/Electronic Signature export	
FMT_MSA.3/Electronic signature export	Le format de la signature en provenance du SCDev est le PKCS#1, ce choix n'est pas paramétrable. Le format final de la signature, est fixé par la politique de signature ; il s'agit du XAdES EPES. La TOE formate la signature XAdES EPES. Le format est conforme au schéma XAdES version 1.3.2
FMT_MSA.1/SCDev signature generation status	Le retour de la signature est fourni par le module de communication avec le SCDev, il n'est pas possible à la TOE d'accéder directement à la valeur de ce code.
FMT_SMF.1/Getting SCDev signature generation	Le résultat de la signature est fourni à la TOE par le module de communication du SCDev. Si l'opération a échoué, aucune valeur de signature n'est retournée.

FCS _COP.1/Hash function	L'algorithme de hachage utilisé par la TOE est fixé par la politique de signature. Il s'agit du SHA-256.
FMT_SMR.1/Security roles	La TOE distingue 2 acteurs humains : • Le signataire qui utilise la TOE directement à chaque signature et se fait reconnaitre en utilisant son propre SCDev et le pin Code associé. • L'administrateur de sécurité n'intervient pas directement dans la TOE Toutefois l'administrateur produit et maintient les politiques de signature utilisées par la TOE, il est authentifié par la TOE au moyen de la signature qu'il applique dans ses politiques de signature.
FIA_UID.2/User identification	La TOE n'est utilisée que par le signataire. Celui-ci s'authentifie au moyen de son PIN code associée au SCDev.
FMT_MTD.1/Document format / viewer association	L'association entre un format de document et le module de visualisation correspondant est un paramétrage statique dans la TOE, il n'est pas modifiable.
FMT_SMF.1/Management of the document format / viewer association	L'association, type de document/module de visualisation, étant statique, elle ne peut être modifiée (cf. FMT_MTD.1/Management of the signature policies et FMT_SMF.1/Management of the signature policies) L'administrateur de sécurité ne dispose d'aucun moyen de modifier cette association.
FMT_MTD.1/Management of the signature policies	L'administration de la politique de signature (création, modification, suppression…) n'est pas réalisée au sein de la TOE, Lorsqu'il produit une politique de signature, l'administrateur de sécurité signe cette politique de signature. Cette signature est contrôlée par la TOE pour autoriser sa prise en compte lors d'une signature. La TOE valide l'origine de la politique par un administrateur de sécurité par cette signature Toutes ces fonctions que réalise l'administrateur de sécurité sont Hors TOE, ainsi lorsqu'une politique de signature est utilisée par la TOE celle-ci est de fait, statique.
FMT_SMF.1/Management of the signature policies	

8 Argumentaire.

8.1 Argumentaire des objectifs de sécurité.

L'argumentaire des objectifs de sécurité est directement celui du profil de protection [PP-01]

8.2 Argumentaire des exigences de sécurité.

L'argumentaire des exigences de sécurité est directement repris du profil de protection [PP-01].

Toutefois certaines exigences ont été modifiées dans le sens d'un renforcement :

- La TOE ne permet pas de signer un document déterminé comme non stable
    - FDP_IFF.1/Document acceptance Simple security attributes
    - FMT_MSA.1/Signer agreement to sign an instable document Management of security attributes
    - FMT_SMF.1/Getting signer agreement to sign an instable document Specification of Management Functions

8.3 Dépendances.

Les dépendances des exigences de sécurité fonctionnelles et de sécurité d'assurance, les dépendances non satisfaites sont repris directement du profil de protection [PP-01].

8.4 Argumentaire pour l'EAL.

Le niveau de cette cible de sécurité est EAL 3 augmenté,
Car c'est le niveau requis par

- Le Référentiel Général de Sécurité pour les services de signature [RGS_A_3]
- le processus de qualification standard [QUA-STD].

8.5 Argumentaire pour les augmentations à l'EAL.

8.5.1 AVA_VAN.3 Focused vulnerability analysis.

Augmentation requise par le processus de qualification standard [QUA-STD].

8.5.2 ALC_FLR.3 Systematic flaw remediation.

Augmentation requise par le processus de qualification standard [QUA-STD].

Annexe A Glossaire.

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 :

- L'identité du prestataire de services de certification électronique ainsi que l'État dans lequel il est établi ;
- Le nom du signataire ou un pseudonyme, celui-ci devant alors être identifié comme tel;
- Le cas échéant, l'indication de la qualité du signataire en fonction de l'usage auquel le certificat électronique est destiné ;
- Les données de vérification de signature électronique qui correspondent aux données de création de signature électronique ;
- L'indication du début et de la fin de la période de validité du certificat électronique ;
- Le code d'identité du certificat électronique ;

- 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 :

- Une mention indiquant que ce certificat est délivré à titre de certificat électronique qualifié ;
- 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 signatures 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, comme des clés cryptographiques privées, utilisés par lui pour créer une signature électronique ;

Données de vérification de signature électronique.

Les éléments, comme 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 conformément à la norme ISO/IEC 9834, et 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

AC	AUTORITÉ DE CERTIFICATION
DN	DISTINGUISH NAME
JVM	JAVA VIRTUAL MACHINE
SCDev	DISPOSITIF DE CRÉATION DE SIGNATURE
SSCD	SECURE SIGNATURE CREATION DEVICE
ST	CIBLE DE SÉCURITÉ (SECURITY TARGET)
TOE	CIBLE D'ÉVALUATION (TARGET OF EVALUATION)
XAdES	XML ADVANCED ELECTRONIC SIGNATURE
ETSI	EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE
CSP	CRYPTOGRAPHIC SERVICE PROVIDER. EN FRANÇAIS, FOURNISSEUR DE SERVICES CRYPTOGRAPHIQUES.
CWA	CEN WORKSHOP AGREEMENTS
PKCS#11	PUBLIC KEY CRYPTOGRAPHY STANDARDS
OID	OBJECT IDENTIFIER, EN FRANÇAIS IDENTIFIANT D'OBJET.
IHM	INTERFACE HOMME/MACHINE
SOF	STRENGTH OF FUNCTION.EN FRANÇAIS « LA FORCE DES FONCTIONS ». CECI CORRESPOND À ÉVALUER LA FORCE THÉORIQUE DES PRIMITIVES, PAR EXEMPLE LA RÉSISTANCE DES PRIMITIVES CRYPTOGRAPHIQUES POUR DES ATTAQUES DE TYPE FORCE BRUTE.

9 Fin du document