Cible de sécurité - Lite

Module de signature client AdSignerWeb

Date de dernière mise à jour : 18/04/2006

Référence : Dictao_ADOSI_CibleDeSecurite_Lite

Références du document

Référence : Dictao_ADOSI_CibleDeSecurite_Lite
Date de dernière mise à jour : 18/04/2006
Version : 5.0 - Lite
Version du logiciel associé : 3.1.800

Etat	Travail (T) :	En cours de validation (ECV) :	Validé (V) : X
Niveau de confidentialité :	Public (P) : X	Diffusion Restreinte (DR) :	Confidentiel (C) :

SOMMAIRE

SOMMAIRE 3

1. ACRONYMES ET ABREVIATIONS 6
1.1 Abréviations 6
1.2 Références 6

2. INTRODUCTION 8
2.1 Identification de la cible de sécurité et de la cible d'évaluation 8
2.2 Vue d'ensemble de la cible de sécurité 8
2.2.1 Présentation de la cible d'évaluation 8
2.2.2 Conformité aux Critères Communs 8
2.2.3 Présentation de la cible de sécurité 9

3. DESCRIPTION DE LA CIBLE D'EVALUATION 10
3.1 Description générale 10
3.2 Périmètre et architecture de la cible d'évaluation 10
3.2.1 Représentation physique 10
3.2.2 Architecture 11
3.2.3 Utilisation de la TOE 13
3.2.4 Cycle de vie du produit 13
3.2.5 Séquencement / exécution du module 14
3.2.6 Problématique du What You See Is What You Sign (WYSIWYS) 14
3.2.7 Contrôle de l'invariance sémantique et présentation du document 15
3.2.8 La politique de signature 15
3.2.9 Les attributs de signature 16
3.2.10 Le format XAdES 16
3.3 Eléments exclus du périmètre d'évaluation 17
3.3.1 La plateforme hôte 17
3.3.2 Le fournisseur de service cryptographique 18
3.3.3 Le dispositif de création de signature 18

4. ENVIRONNEMENT DE SECURITE DE LA CIBLE D'EVALUATION 19
4.1 Description des biens sensibles 19
4.1.1 Biens sensibles protégées par la TOE 19
4.1.2 Biens sensibles de la TOE 20
4.2 Description des sujets 21
4.3 Hypothèses 22
4.3.1 Hypothèses sur l'environnement d'utilisation 22
4.3.2 Hypothèses sur le contexte d'utilisation 24

4.4 Menaces 25
4.5 Politiques de sécurité organisationnelles 25
4.5.1 Politiques relatives à la validité de la signature créée 25
4.5.2 Contrôle de l'invariance de la sémantique du document 25
4.5.3 Présentation du document et des attributs de signature au signataire 26
4.5.4 Conformité aux standards 26
4.5.5 Interaction avec le signataire 26
4.5.6 Divers 26

5. OBJECTIFS DE SECURITE 28
5.1 Objectifs de sécurité de la cible d'évaluation 28
5.1.1 Objectifs généraux 28
5.1.2 Interaction avec le signataire 28
5.1.3 Application d'une politique de signature 28
5.1.4 Protection des données 29
5.1.5 Opérations cryptographiques 29
5.1.6 Contrôle de l'invariance de la sémantique du document 29
5.1.7 Présentation du ou des documents à signer 30
5.1.8 Vérification du bon fonctionnement du SCDev 30
5.2 Objectifs de sécurité pour l'environnement 30
5.2.1 Machine hôte 30
5.2.2 Objectifs relatifs au SCDev et à son environnement 31
5.2.3 Dispositif de création de signature 31
5.2.4 Présence du signataire 32
5.2.5 Présentation/sémantique invariante du ou des documents à signer 32
5.2.6 Divers 32

6. EXIGENCES DE SECURITE 34
6.1 Exigences fonctionnelles de sécurité de la TOE 34
6.1.1 Contrôle de l'invariance de la sémantique du document 34
6.1.2 Interaction avec le signataire 37
6.1.3 Règles de validation 37
6.1.4 Application de la politique de signature et génération de la signature numérique 39
6.1.5 Retour de la signature électronique 41
6.1.6 Opérations cryptographiques 43
6.1.7 Identification et authentification de l'utilisateur 43
6.1.8 Administration de la TOE 43
6.2 Exigences de sécurité d'assurance pour la TOE 44

7. SPECIFICATION GLOBALES DE LA CIBLE D'EVALUATION 45
7.1 Fonction de sécurité de la TOE 45
7.1.1 F. Signature 45
7.1.2 F.Contrôle_Invariance_Sémantique 46
7.1.3 F.Sélection_Certificat 46

7.1.4 F.Présentation_Document 46
7.1.5 F.Administration 46
7.1.6 F.Applique_Politique_Signature 46
7.1.7 F.Transfert_vers_SCDev 47
7.1.8 F.Présentation_attributs 47
7.2 Mesures d'assurance pour la cible d'évaluation 48
7.2.1 Développement 48
7.2.2 Support au développement et livraison 49
7.2.3 Tests et analyse de vulnérabilité 50
7.2.4 Guides 50
7.2.5 Couverture des mesures d'assurance 51
8. CONFORMITE AU PROFIL DE PROTECTION 52
8.1 Référence du Profil de protection 52
8.2 Modifications apportées par rapport au Profil de protection 52
8.2.1 Les sujets 52
8.2.2 La présentation de document 53
8.2.3 Le contrôle d'invariance sémantique 55
8.2.4 Signature au format XAdES 56
8.2.5 Vérification du format PKCS#1 56
8.2.6 Politique de signature 57
8.2.7 Signature d'un seul document 58
8.2.8 Contexte d'utilisation 58
8.2.9 Autres assignements 59
8.2.10 Autres raffinements 59
8.2.11 Autres biens 60
8.3 Récapitulatif des modifications 60
9. ARGUMENTAIRE 66
9.1 Argumentaire pour l'ajout des exigences FDP_MRU.1 66
9.1.1 Définition du composant 66
9.1.2 Argumentaire pour l'ajout 67
9.1.3 Testabilité du composant 67
9.1.4 Applicabilité des exigences d'assurance 67
10. ANNEXE B – DEFINITIONS 68

1. ACRONYMES ET ABREVIATIONS

1.1 Abréviations

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

1.2 Références

Référence	Document
[CC]	Critères Communs : • Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. référence CCIMB-2004-01-001 Version 2.2 January 2004 • Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements. référence CCIMB-2004-01-002 Version 2.2 January 2004 • Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements. référence CCIMB-2004-01-003 Version 2.2 January 2004
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology référence CCIMB-2004-01-004 Version 2.2 January 2004
[CRYPT_STD]	Mécanismes cryptographiques _ Règles et recommandation concernant le choix et dimensionnement des mécanismes cryptographiques de niveau de robustesse *standard* et *renforcé* Référence 001064/SGDN/DCSSI/DSD/AsTec Version 1.0 mai 2004 DCSSI
[EXT_DCSSI_PP]	Profil de protection « Application de création de signature »

	référence PP-ACSE version 1.0
[EXT_TS_101_733]	Electronic signature formats version 1.5.1 15 décembre 2003 ETSI standard
[EXT_TS_101_862]	Qualified Certificate Profile version 1.3.1 Mars 2004 ETSI Standard
[FIPS 180-2]	Secure Hash Standard (+ Change Notice to include SHA-224) Federal Information Processing Standards (FIPS) Publication 180-2 February 2004
[QUA_STD]	Processus de qualification d'un produit de sécurité – Niveau standard. référence 001591/SGDN/DCSSI/SDR Version 1.0 juillet 2003 DCSSI
[XAdES]	XML Advanced Electronic Signatures référence ETSI TS 101 903 version 1.1.1 et version 1.2.2
[IGS]	Guide d'intégration référence dictao_adosi_gu01 version 4.5
[ST]	Module de signature client AdSignerWeb Cible de sécurité référence Dictao_ADOSI_CibleDeSecurité version 5.0

2. INTRODUCTION

2.1 Identification de la cible de sécurité et de la cible d'évaluation

Ce document constitue la cible de sécurité de AdSignerWeb "Module de signature client AnySign".

- Auteur : **Dictao**
- Titre de la ST : **Module de signature client AdSignerWeb – Cible de sécurité - Lite**
- Version de la ST : **5.0 - Lite**
- Identifiant de la TOE : **AdSignerWeb**
- Version de la TOE : **3.1.800**
- Plateformes : **les plateformes sur lesquelles la TOE est évaluée sont identifiées au paragraphe 3.3.1**
- Mots clé : **Signature électronique, Application de signature électronique, Application de création de signature électronique, Applet**

La version de la cible de sécurité utilisée pour l'évaluation est sous la référence [ST] :

- Titre de la ST : **Module de signature client AdSignerWeb – Cible de sécurité**
- Version de la ST : **5.0**
- Référence : **Dictao_ADOSI_CibleDeSecurite**

2.2 Vue d'ensemble de la cible de sécurité

2.2.1 Présentation de la cible d'évaluation

La cible d'évaluation définie dans le présent document est constituée d'un module de signature électronique au format XAdES (1.1.1 ou 1.2.2), packagé sous forme d'une Applet Java et d'un module ActiveX. Ce module s'exécute dans un navigateur Internet (en dehors du périmètre de la cible d'évaluation).

Le chapitre 3 décrit et présente précisément la cible d'évaluation.

Nom de l'objet : AdSignerWeb

Numéro de la version évaluée : 3.1.800

2.2.2 Conformité aux Critères Communs

Conformité aux CC

La présente cible de sécurité est conforme à la partie 2 des Critères Communs étendue du composant FDP_MRU.1 (cf. §9.1) et à la partie 3 des Critères Communs, Version 2.2 avec les interprétations suivantes :

- RI # 86 – Role of Sponsor ;
- RI # 137 – Rules governing binding should be specifiable ;
- RI # 146 – C&P elements include characteristics ;
- RI # 192 – Sequencing of sub-activities ;

- RI # 220 – FCS_CKM/COP dependency on FDP_ITC.1 ;
- RI # 227 – CC Part2 F.12 user notes ;
- RI # 228 – Inconsistency between FDP_ITC and FDP_ETC ;
- RI # 232 – FDP_ROL statement ;
- RI # 243 – Must Test Setup And Cleanup Code Run Unprivileged?.

Conformité à un PP

La Cible de sécurité est conforme au profil de protection « Application de création de signature » [EXT_DCSSI_PP].

Les modifications apportées par rapport au profil de protection sont été indiquées dans la cible de sécurité par bleu souligné pour les ajouts et ~~orange barré~~ pour les suppressions.

Les spécificités de la présente cible de sécurité vis-à-vis du profil de protection sont résumées au chapitre 8.

Niveau d'assurance

Le niveau d'assurance visé est le niveau EAL3 augmenté des composants d'assurance ADV_IMP.1*, ADV_LLD.1*, ALC_FLR.3, ALC_TAT.1*, AVA_VLA.2.

Note : Ce niveau d'assurance correspond aux exigences définies par la DCSSI pour le niveau de qualification au niveau standard. [QUA_STD]

Niveau de résistance

Le niveau de résistance visé pour les fonctions de sécurité de la TOE est « SOF élevé ».

2.2.3 Présentation de la cible de sécurité

La cible de sécurité définit les bases pour l'évaluation du module AdSigner, au travers du plan suivant :

- La description informelle de la cible d'évaluation au chapitre 3 ;
- La description de l'environnement dans lequel la TOE est utilisée (au chapitre 4), au travers de la définition des hypothèses sur l'environnement de la TOE, des menaces que la TOE devra contrer et des contraintes (ou politiques de sécurité organisationnelles) qu'elle doit respecter ;
- Le chapitre 5 identifie les objectifs de sécurité à satisfaire par la TOE et son environnement ;
- La présentation des exigences de sécurité fonctionnelles et d'assurance (cf chapitre 6) que devra respecter la TOE afin de répondre à ses objectifs de sécurité ;
- Puis la définition des fonctions de sécurité de la TOE et des mesures d'assurance (chapitre 7) montrant comment la TOE répond aux exigences présentées précédemment ;
- Enfin, le chapitre 8 présente l'argumentaire de conformité au profil de protection [EXT_DCSSI_PP] et le chapitre 9 démontre, au travers aussi d'un argumentaire, la complétude et la cohérence de la cible de sécurité dans son ensemble, de la définition de son environnement jusqu'à la présentation de ses fonctions de sécurité et mesures d'assurance.

* Uniquement pour les fonctions cryptographiques spécifiées au travers des exigences de la classe FCS au paragraphe 6.1.6.

3. DESCRIPTION DE LA CIBLE D'EVALUATION

Après une description générale, ce chapitre décrit le périmètre et l'architecture de la cible d'évaluation, puis son environnement.

Les plateformes utilisées pour l'évaluation sont présentées au paragraphe 3.3.1. Par la suite, nous entendrons par plateforme le triplet machine, système d'exploitation et navigateur Internet.

3.1 Description générale

La cible d'évaluation (ou TOE - Target Of Evaluation) est le module AdSignerWeb permettant la création de signatures électroniques au format XAdES (version 1.1.1 ou 1.2.2), en s'appuyant sur un dispositif de création de signature externe (hors périmètre d'évaluation). Signant les documents sous forme HTML et texte brut, en effectuant lui-même l'interprétation du document HTML et son affichage, le module AdSignerWeb peut être utilisé par exemple pour la signature de demande de transaction financière en ligne, mais aussi la signature de déclarations et formulaires (téléTVA, téléIR, ...).

Il fait partie d'un système global de création de signature électronique, incluant l'application et le dispositif de création de signature[1]. 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, un token USB ou encore sous forme logicielle.

La TOE est exécutée suite à son appel par une "page web" (nommée par la suite application appelante). Son exécution se fait au travers du navigateur Internet (hors périmètre d'évaluation) dans lequel la page web se trouve. Le document à signer est passé à la TOE par la page web sous forme d'un paramètre. Plusieurs autres informations sont aussi transmises en paramètre (cf §3.2.5).

3.2 Périmètre et architecture de la cible d'évaluation

3.2.1 Représentation physique

La TOE est composée de deux fichiers : un fichier .cab et un fichier .jar. Correspondant à des environnements d'exécution différents, ils effectuent cependant les mêmes opérations. Ainsi :

- L'élément ActiveX (fichier .cab) s'exécute en environnement Windows et Internet Explorer ;
- et l'applet Java dédiée à la JVM Sun (fichier .jar) s'exécute sous de nombreux types de systèmes d'exploitation et navigateurs (cf §3.3.1), à condition que la JVM de Sun soit installée sur la machine hôte.

C'est l'application appelante qui détermine sur quelle environnement va être exécutée la TOE et donc détermine à quel élément (fichier) faire appel. Cette « détection d'environnement » est hors périmètre d'évaluation, toutefois, son algorithme est fourni dans le guide de développement.

Les plateformes (hors périmètres) sur lesquelles est évalué le produit sont définies au paragraphe 3.3.1.

En environnement d'utilisation normal, les fichiers se trouvent sur un serveur Web. Ils sont téléchargés lors de leur utilisation. Dans le cadre de l'évaluation, les trois fichiers seront déjà installés sur la machine hôte, considérant que le téléchargement est hors périmètre d'évaluation.

[1] Il sera aussi nommé SCDev dans la suite du document, pour Signature Creation Device.

3.2.2 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 : la détection d'environnement par l'application appelante, le middleware de communication avec le SCDev et le SCDev lui-même.

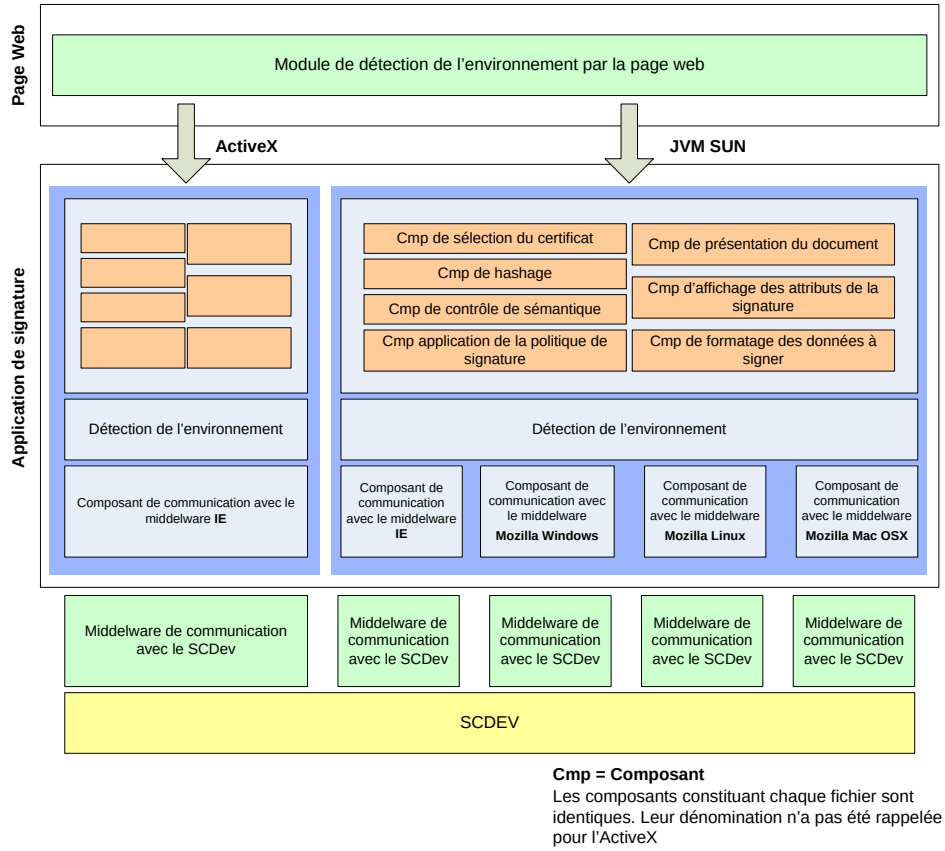

Figure 1 - Architecture interne de la TOE

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

- La détection d'environnement par l'application appelante ;
- L'appel à l'un des trois fichiers ;
- Trois sous-ensembles représentant chacun des trois 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.

3.2.2.1 Composant de contrôle de l'invariance de la sémantique du document

La TOE permet de signer des documents au format texte brut et HTML :

- Le texte brut est invariant dans le temps par définition ;
- Pour un document HTML, elle contrôle l'invariance de la sémantique du document en s'appuyant sur la définition des balises HTML définies dans le guide d'intégration [IGS].

Pour plus de détails sur le contrôle de sémantique, le lecteur peut se reporter au paragraphe 3.2.7.

3.2.2.2 Composant de présentation de documents

La TOE affiche le contenu du document à signer soit au travers d'un cadre de texte lorsque le document est en texte brut, soit en interprétant et affichant le contenu HTML (restreint) du document.

Lorsque la TOE ne peut afficher le document, la signature est arrêtée.

3.2.2.3 Composant d'application de la politique de signature

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

Le paragraphe 3.2.8 présente les informations constituant une politique de signature. Ils sont optionnels, des valeurs par défauts leur étant attribués lorsque l'application appelante ne les définit pas.

3.2.2.4 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 §3.3.2), 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 CN (Common Name) du sujet certificat ;
- La date d'émission du certificat ;
- Le CN de l'Autorité de certification émettrice du certificat.

3.2.2.5 Composant d'affichage des attributs de la signature

Ce composant présente les attributs de signature au signataire, sur sa demande. Les informations affichées sont détaillées au paragraphe 3.2.9.

3.2.2.6 Composant de formatage des données à signer

Ce composant construit la structure de signature électronique au format XML XAdES version 1.1.1 ou 1.2.2 selon la demande de l'application appelante.

3.2.2.7 Composant de hashage

Le composant de hachage permet de calculer le condensat des données formatées selon l'algorithme SHA-1 et SHA-256.

3.2.2.8 Composant de détection d'environnement

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

3.2.2.9 Composant de communication avec le dispositif de création de signature

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

- Obtenir du SCDev les références des certificats utilisables par le signataire, ou les certificats eux-mêmes ;
- Indiquer au SCDev la clé de signature à activer ;
- Transférer 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 ;
- Gérer (refermer) une session avec le SCDev.

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. »

3.2.3 Utilisation de la TOE

La TOE est présente sur un serveur web. Avant d'appeler le module, la page web appelante doit détecter l'environnement dans lequel le module sera exécuté (type de machine, système d'exploitation et navigateur).

La page web appelle ensuite le fichier du module AdSignerWeb qui saura être interprété correctement par l'environnement dans lequel il s'exécutera.

Ceci amène à la cinématique suivante (en dehors du périmètre d'évaluation) :

- La détection de l'environnement par l'application appelante ;
- L'appel au fichier du module AdSignerWeb correspondant à l'environnement, en lui transmettant les paramètres à utiliser pour le processus signature ;
- Le téléchargement du fichier par le navigateur Internet ;
- L'installation sur la machine hôte du fichier.

Dans le cadre de l'évaluation, le serveur web est présent sur la même machine hôte que l'application appelante, et l'installation du fichier est déjà effectuée.

3.2.4 Cycle de vie du produit

Le cycle de vie du produit est le suivant :

Phase	Description	Acteur
Spécification	Spécification du produit	Dictao
Développement	Développement du produit	Dictao
Tests	Tests et recette	Dictao

Livraison	Livraison du produit et de sa documentation	Développeur de l'application appelante
Intégration	Intégration du produit dans une application web	Développeur de l'application appelante
Installation sur le serveur	Chargement sur le serveur web du produit	Développeur de l'application appelante
Téléchargement et Installation sur la machine hôte (automatique)		Utilisateur final
Utilisation		Utilisateur final

3.2.5 Séquencement / exécution du module

Les opérations effectuées par le module respectent la cinématique suivante :

1. Le module AdSignerWeb est appelé par l'application appelante (page web), avec en paramètres:
   - le document à signer, sous forme de données brutes encodées en base64
   - la référence de la politique de signature (cf paragraphe 3.2.8)
   - 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 manière dont les données doivent être interprétées par la TOE (soit HTML soit texte brut).
   - la version de la signature XAdES à générer. Les versions possibles sont :
     - 1.1.1
     - 1.2.2 (version par défaut si aucune version n'est spécifiée)
2. le module analyse de contenu du document si ce dernier est au format HTML
3. s'il contient des balises non reconnue, la signature est arrêtée
4. il affiche ensuite à l'utilisateur :
   - le document à signer
   - la liste des certificats répondant aux contraintes introduites par la politique de signature est affichée au signataire. Cette liste est récupérée du SCDev à travers le fournisseur d'accès aux services cryptographiques
   - le type d'engagement si ce dernier a été passé en paramètre
5. il présente sur demande du signataire le récapitulatif des attributs de signature (cf paragraphe 3.2.9)
6. après sélection du certificat et demande explicite du signataire, la TOE :
   - formate les données au format XAdES
   - calcule le condensat des données à signer formatées
   - puis envoie au dispositif de création de signature le condensat, accompagné de la référence vers la clé privée à utiliser
7. le dispositif renvoie le chiffré du condensat
8. la TOE l'intègre ensuite à la signature XAdES et renvoie l'ensemble à l'application appelante.

3.2.6 Problématique du What You See Is What You Sign (WYSIWYS)

A l'instar du profil de protection [EXT_PP_DCSSI], 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.

AdSignerWeb réalise lui-même l'ensemble de ces trois fonctions.

3.2.7 Contrôle de l'invariance sémantique et présentation du document

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

La TOE accepte de signer les documents sous forme texte brut (dont le contenu ne peut varier par construction) et au format HTML.

Afin de s'assurer de l' « invariance sémantique » du document HTML à signer, la TOE n'accepte que certaines balises du langage HTML. Ces balises sont présentées dans le guide d'intégration [IGS].

Il faut noter toutefois que la TOE présente elle-même le document et que par conséquent, si une balise HTML est non reconnue, la TOE ne pouvant l'afficher, elle refusera de procéder à sa signature. Par construction AdSignerWeb ne pourra donc jamais signer un document dont la sémantique est détectée instable. C'est pourquoi la politique de signature ne comporte pas de paramètre « permettre ou non de signer un document instable ».

3.2.8 La politique de signature

La politique de signature comprend les informations suivantes :

- la liste des ACs autorisées : seuls les certificats issus de ces ACs sont proposées au signataire ;
- la clé publique du certificat à afficher : seul le certificat avec la clé publique indiquée est proposé à l'utilisateur ;
- la référence de la politique de signature : cette référence est constituée de l'identifiant (URL ou OID) du document décrivant la politique de signature ainsi que du condensât de ce document. Le document reprend entre autre les paramètres de politique qui ont été transmis au module AdsignerWeb ;
- la date de filtrage : seuls les certificats valides à la date indiquée sont proposés au signataire ;
- le type d'engagement : si présent, le type d'engagement est présenté à l'utilisateur avant la création de la signature et est ensuite inclus dans les données à signer ;
- le rôle du signataire : si présent, le rôle du signataire est inclus dans les données à signer ;
- le lieu de signature : si présent, le lieu de signature est inclus dans les données signées par le signataire ;
- Le certificat est utilisable ou non pour des applications de non répudiation :
  - 1 : requérir la non-répudiation
  - 0 : ne pas requérir la non-répudiation
- Le certificat est déclaré qualifié ou non [EXT_TS_101_862] :

- 1 : le certificat doit être un certificat déclaré comme qualifié
- 0 : cette condition n'est pas requise

- Le certificat déclare que la clé privée associée est protégée ou non par un SSCD [EXT_TS_101_862] :
  - 1 : le certificat doit déclarer que la clé privée associée est protégée par un SSCD
  - 0 : cette condition n'est pas requise

Dans le cas où l'application appelante ne définit pas de politique de signature, les valeurs suivantes sont utilisées :

- liste des ACs autorisées : toutes
- clé publique du certificat : aucune
- date de filtrage : la date du jour sur le poste client est utilisée pour le filtrage
- le type d'engagement : aucun
- rôle du signataire : aucun
- lieu de signature : aucun
- ne pas requérir la non-répudiation : 0
- niveau de qualification des certificats : 0 (certificat non qualifié)

3.2.9 Les attributs de signature

Les attributs de signature sont donnés ci-dessous. Ils sont présentés au signataire sur sa demande.

- la référence de la politique de signature. Si une URL est indiquée par l'application, un lien actif vers cette page est présenté au signataire ;
- le type d'engagement du signataire (si spécifié par l'application appelante) ;
- le rôle du signataire (si spécifié par l'application appelante) ;
- la référence au certificat de signature sélectionné par le signataire (Le DN du certificat, son numéro de série, le DN de l'AC émettrice ainsi que la période de validité du certificat) ;
- la date de signature. Cette date est récupérée depuis la machine hôte. Elle constitue la date « déclarée » de signature et ne peut être considérée comme un horodatage ;
- le lieu de signature (si spécifié par l'application appelante).

3.2.10 Le format XAdES

La syntaxe XML et les règles de traitement pour créer et représenter des signatures digitales sont donnés 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) prolonge 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 au format DSig sont :

- la date déclarée de signature ;
- le certificat ou une référence vers le certificat de signature ;
- la référence de la politique de signature sous forme d'un hash et d'une URL ou OID ;
- le lieu de la signature (optionnel) ;

- le rôle du signataire (optionnel).

La syntaxe XML de la signature est conforme au standard XML version 1.0.

3.3 Eléments exclus du périmètre d'évaluation

L'environnement de la cible d'évaluation est composé des 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.

3.3.1 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 ;
- le navigateur Internet.

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
- Configurations logicielles suivantes :

	Internet Explorer v6.0 SP2 JRE v1.5.0_06	Mozilla v1.7.12 JRE v1.5.0_06	Firefox v1.5 JRE v1.5.0_06
Windows XP	❑ Module ActiveX ❑ Module Java Sun	❑ Module Java Sun	❑ Module Java Sun
Windows Server 2003	❑ Module ActiveX		
Fedora Core 4 (Linux 2.6.12)		❑ Module Java Sun	❑ Module Java Sun

- Les dispositifs de création de signature utilisés sont :
  - SCDev logiciel du Navigateur
  - Carte à puce Cyberflex Access e-gate 32K USB de Axalto (sur environnement Windows XP / Internet Explorer)

➢ **Mac**

- Matériel :
  - CPU : Power/PC G4 1,25 GHz / RAM : 768 Mo / Disque dur : 20 Go

- Configurations logicielles suivantes :

	Mozilla v1.7.12 JRE v1.3.1	Firefox v1.5 JRE v1.4.2
MAC OS X (10.3)	❑ Module Java Sun	❑ Module Java Sun

- Le dispositif de création de signature utilisé étant :
  - SCDev logiciel du Navigateur

Toutefois, le module de signature est prévu pour fonctionner correctement sur les plateformes suivantes :

	IE6	IE5.5	IE5.0	Ns7.1	Ns7.02	Mz 1.0-1.2	Mz 1.3-1.7	Fx 1.0-1.5
Windows XP								
Windows 98								
Windows 95								
Windows NT4								
Windows Me								
Windows 2000								
MAC OS X (10.1)								
MAC OS X (10.2)								
MAC OS X (10.3)								
Linux 2.4.x								

Tableau 1 - plateformes sur lesquelles le module peut fonctionner (mais seule les configurations indiquées au tableau précédent sont évaluées)

3.3.2 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 peut se présenter sous la forme :

- d'un CSP (Cryptographic Service Provider) dans le cas d'une utilisation avec Internet Explorer. Ce CSP communique directement avec le dispositif de création de signature ;
- d'une librairie NSS (Netscape Security Service) dans le cas d'une utilisation avec les navigateurs Mozilla ou Netscape. Ce composant communique avec la librairie PKCS#11 du dispositif de création de signature ;

3.3.3 Le dispositif de création de signature

Les dispositifs de création de signature supportés par la TOE sont ceux disposant d'un fournisseur de service cryptographique, sous forme de CSP (Cryptographic Service Provider), de librairie PKCS#11, supporté par la plateforme hôte.

Parmi ces dispositifs, on trouve :

- les tokens USB
- les cartes à puce
- un module logiciel CryptoAPI
- etc...

4. ENVIRONNEMENT DE SECURITE DE LA CIBLE D'EVALUATION

4.1 Description des biens sensibles

Tous les biens sensibles sont à protéger en intégrité.

4.1.1 Biens sensibles protégées par la TOE

4.1.1.1 Document à signer

B1. Document_à_signer

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

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

Le document à signer est constitué de données brutes passées par l'application appelante au module de signature.

4.1.1.2 Représentations des données à signer

B2. Données_à_signer

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

Elles sont fournies à la TOE par l'application appelante et comprennent :

- Document à signer (données brutes envoyées à la TOE)
- Les attributs de la signature sélectionnés explicitement par l'application appelante ou implicitement par la TOE

Les attributs de la signature comportent les données suivantes :

- Le certificat du signataire
- Une référence non ambiguë du certificat du signataire (DN de l'AC et numéro de série, condensât du certificat)
- La référence de la politique de signature
- Le type d'engagement (si spécifié)
- Le rôle du signataire (si spécifié)
- Le lieu présumé de la signature (si spécifié)
- La date et l'heure présumées de la signature

B3. Données_à_signer_formatées

Ces données correspondent à un formatage XAdES des données_à_signer (enveloppe).

B4. Condensé_des_données_à_signer

Cette donnée est le condensé des *Données_à_signer_formatées*.

B5. Condensé_formaté

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

Le formatage consiste en l'ajout de l'identifiant (OID) de l'algorithme de hashage mis en œuvre.

4.1.1.3 Données retournées par la TOE

B6. Signature_électronique

La signature électronique est une enveloppe comprenant :

- Le condensé de l'ensemble des données à signer ;
- La signature numérique ;
- Et comprenant aussi entre autre (requises par le standard XAdES) :
  - L'ensemble des données signées ;
  - La méthode de *canonicalization* ;
  - L'algorithme de signature ;
  - Le certificat du signataire.

4.1.2 Biens sensibles de la TOE

B7. Politique_de_signature

La TOE réalise la signature selon une politique de signature, comprenant les éléments suivants :

- la liste des ACs autorisées
- la clé publique du certificat à afficher
- la référence de la politique de signature
- la date de filtrage
- le type d'engagement
- le rôle du signataire
- le lieu de signature
- le niveau de qualification requis pour les certificats

B8. Services

Ce bien représente le code exécutable implémentant les services rendus par la TOE

B9. Correspondance_Entre_Représentation_De_Données

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

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

B10. Correspondance_FormatDoc_Application

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

Note :

La TOE affiche elle-même le document à signer. La correspondance est effectuée en fonction du paramètre d'appel.

4.2 Description des sujets

S1. Signataire

Le signataire interagit avec la TOE pour signer un ~~ou plusieurs~~ document~~s~~ selon ~~une~~ la politique de signature définie par l'application appelante.

~~**Administrateur_de_securité**~~

~~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~~
- ~~Gestion de la liste des politiques de signature utilisables par la TOE~~

~~*Note d'application*~~

~~Le rôle d'administrateur de sécurité de la TOE est bien distingué du rôle d'administrateur de la machine sur laquelle elle s'exécute (voir l'hypothèse H1.Machine_Hôte).~~

Note :

Dans le cas de la présente cible d'évaluation, l'administrateur de sécurité est représenté par les trois rôles ci-après.

S2. Application_Appelante

L'application appelante administre la TOE au travers des paramètres d'entrée qu'elle lui transmet. Ainsi l'application appelante est en charge de transmettre à la TOE :

- Le contenu du document à signer
- La politique de signature à appliquer par la TOE

S3. Administrateur_Application_Appelante

L'administrateur de sécurité de l'application appelante est en charge des opérations suivantes :

- Gestion de la liste des politiques de signature utilisables par la TOE

Note :

il ne doit pas être confondu avec l'administrateur de sécurité de la TOE défini dans le profil de protection, puisque cet administrateur gère l'application appelante et non la TOE directement. C'est l'application appelante qui transmet les paramètres à la TOE.

Remarque :

Cet administrateur peut ne pas être nécessaire lorsque l'application appelante n'est pas paramétrable. Dans ce cas, cet administrateur est le développeur de l'application appelante.

Note d'application

Ce rôle est bien distingué du rôle d'administrateur de la machine sur laquelle la TOE s'exécute (voir l'hypothèse H1.Machine_Hôte).

S4. Developpeur_Application_Appelante

Le développeur de l'application appelante ne joue un rôle sécuritaire qu'à deux niveaux :

- Lorsqu'il développe l'application appelante
- Lorsque l'application appelante est non paramétrable, puisque dans ce cas il est aussi l'administrateur de l'application appelante.

4.3 Hypothèses

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

4.3.1 Hypothèses sur l'environnement d'utilisation

4.3.1.1 Hypothèses sur la machine hôte

H1. 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 en 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:

1. la machine hôte est protégée contre les virus
2. 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
3. l'accès aux fonctions d'administration de la machine hôte est restreint aux seuls administrateurs de celle-ci (différenciation compte utilisateur/administrateur)
4. l'installation et la mise à jour de logiciels sur la machine hôte est sous le contrôle de l'administrateur
5. le système d'exploitation de la machine hôte refuse l'exécution d'applications téléchargées ne provenant pas de sources sûres

Note d'application :

Le rôle d'administrateur de la machine hôte mentionné ci-dessus est à différencier par rapport au rôle d'administrateur de sécurité de ~~la TOE~~ l'application appelante qui a des prérogatives particulières vis-à-vis de la gestion des biens sensibles de la TOE et de l'application appelante ~~et~~ ainsi que de ~~ses~~ leurs paramètres de configuration.

4.3.1.2 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.

H2. 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:

1. Biens relatifs à la génération de la signature
   a. la(les) clé(s) privée(s) du signataire, protégées en confidentialité et en intégrité
   b. le(s) certificat(s) du signataire, protégés en intégrité, à défaut une référence non ambigue à ce(s) certificat(s),
   c. l'association clé privée/certificat, protégée en intégrité
2. Biens relatifs à l'authentification du signataire
   d. les données d'authentification du signataire, protégées en intégrité et en confidentialité.
   e. l'association entre des données d'authentification et le couple clé privée/certificat, protégée en intégrité

H3. 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.

H4. 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.

4.3.1.3 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 :~~

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

Note :

La TOE effectue elle-même l'affichage.

~~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.~~

Note :

La TOE effectue elle-même l'affichage du document. Toutefois, il faut noter que la TOE ne permet pas la contre-signature.

4.3.1.4 Hypothèse concernant l'invariance de la sémantique du document

~~H.Contrôle_Invariance_Sémantique_Document~~

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

~~analyse à la TOE.~~

Note :

Dans le cas de la présente cible d'évaluation, le contrôle de l'invariance sémantique est réalisé par la TOE.

4.3.2 Hypothèses sur le contexte d'utilisation

H5. 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.

H6. Application_Appelante_Sûre

L'application appelante de la TOE (S2.Application_Appelante) est supposée être de confiance.

H7. Développeur_Administrateur_sûr

Le développeur de l'application appelante de la TOE et son administrateur (S4.Developpeur_Application_Appelante et S3.Administrateur_Application_Appelante) sont supposés être de confiance, formés à l'utilisation de la TOE et disposant des moyens nécessaires à la réalisation de son activité.

~~**H.Administrateur_De_Sécurité_Sûr**~~

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

Note :

Dans le contexte de l'application AdSignerWeb, l'administrateur de sécurité de la TOE n'est pas seulement un individu, c'est pourquoi l'hypothèse H.Administrateur_De_Sécurité_Sûr du profil de protection a été scindée en deux : H6.Application_Appelante_Sûre et H7.Développeur_Administrateur_sûr.

H8. Intégrité_Services

L'environnement de la TOE est supposé fournir à ~~l'administrateur de sécurité~~ l'application appelante (S2.Application_Appelante) et/ou son administrateur (S3.Administrateur_Application_Appelante) les moyens de contrôler l'intégrité des services et des paramètres de la TOE.

H9. Politique_Signature_D'Origine_Authentique

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

H10. Communication_Web

On suppose que la communication entre la machine hôte sur laquelle s'exécute la TOE, et le serveur web depuis lequel sont chargées l'application appelante et la TOE, garantit la protection en intégrité des paramètres transmis à la TOE.

H11. Serveur_Web

On suppose que le serveur sur lequel sont stockées la TOE, l'application appelante (page

web, cf §3.1) est protégé de manière à garantir l'intégrité de la TOE et de l'application appelante.

On suppose que les mesures suivantes sont appliquées:

1. le serveur est protégé contre les virus
2. l'accès physique au serveur est protégé
3. les échanges entre le serveur et d'autres machines via un réseau ouvert sont contrôlés par un pare feu contrôlant et limitant les échanges
4. l'accès aux fonctions d'administration du serveur est restreint aux seuls administrateurs de celui-ci (remarque : l'administrateur de l'application appelante et celui du serveur peuvent être deux personnes distinctes)
5. l'installation et la mise à jour de logiciels sur le serveur est sous le contrôle de l'administrateur du serveur

4.4 Menaces

Il n'y a aucune menace que la TOE doit contrer.

4.5 Politiques de sécurité organisationnelles

4.5.1 Politiques relatives à la validité de la signature créée

P1. 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.

P2. 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.

P3. Conformité_Attributs_Signature

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

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

4.5.2 Contrôle de l'invariance de la sémantique du document

P4. Sémantique_Document_Invariante

La TOE doit déterminer si la sémantique du document est invariante.

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

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

- ~~Soit la politique de signature impose de stopper le processus de signature.~~
- ~~Soit la politique de signature ne l'impose pas, et dans ce cas la TOE~~

doit informer le signataire et celui-ci peut alors décider d'outrepasser l'avertissement.

Note :

Par construction, la TOE ne peut signer de document dit instable (cf §3.2.7).

4.5.3 Présentation du document et des attributs de signature au signataire

P5. Possibilité_De_Présenter_Le_Document

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

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

P6. Présentation_Attributs_De_Signature

La TOE doit permettre de présenter les attributs de signature au signataire.

4.5.4 Conformité aux standards

P7. Algorithme_De_Hachage

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

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

4.5.5 Interaction avec le signataire

P8. Signature_De_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.

Note : La TOE ne permet de signer qu'un seul document à la fois.

P9. Arrêt_Processus_Signature

Le signataire doit pouvoir arrêter le processus de signature à tout moment, avant l'activation de la clé de signature

P10. 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.

4.5.6 Divers

P11. 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.

P12. Export_Signature_Electronique

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

- 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 de la politique de signature appliquée

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

P13. Administration

La TOE doit permettre à ~~l'administrateur de sécurité~~ l'application appelante (S2.Application_Appelante) de gérer (ajouter/supprimer) les politiques de signature [B7.Politique_de_signature] ~~et la table de correspondance entre les applications de visualisation et les formats de documents en entrée de la TOE [B10.Correspondance_FormatDoc_Application]~~.

Note :

Bien que ce soit l'administrateur de l'application appelante qui configure l'application et donc ces paramètres, c'est celle-ci qui les transmet à la TOE.

P14. Vérification_Fonctionnement_SCDev

La TOE doit s'assurer que les données renvoyées par le SCDev constituent bien une signature numérique au format PKCS#1.

5. OBJECTIFS DE SECURITE

5.1 Objectifs de sécurité de la cible d'évaluation

5.1.1 Objectifs généraux

O1. 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

O2. Présentation_Conforme_Des_Attributs

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

O3. 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.

O4. 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.

O5. Document_A_Signer

Après que le signataire ait donné son consentement pour signature, la TOE devra garantir que ~~l'ensemble des~~ le document~~s~~ effectivement traité~~s~~ correspond exactement ~~à l'ensemble des~~ au document~~s~~ à signer sélectionné~~s~~.

~~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.~~

Les attributs de signature utilisés pour la signature du document doivent être ceux définis par le signataire.

5.1.3 Application d'une politique de signature

O6. 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.

O7. Validité_Du_Certificat

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

Note d'application :

La référence de temps utilisée pour ce faire est soit celle fournie par l'application appelante, soit celle fournie par le système d'exploitation de la machine hôte si l'application ne précise aucune date.

O8. 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.

O9. Export_Signature_Electronique

A l'issue du processus de signature, la TOE devra transmettre au signataire la signature électronique au format XAdES, comprenant ~~au moins~~ entre autre :

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

5.1.4 Protection des données

O10. Administration

La TOE devra permettre à ~~l'administrateur de sécurité~~ l'application appelante (S2.Application_Appelante) de gérer (ajouter/supprimer) les politiques de signature [B7.Politique_de_signature] ~~et la table de correspondance entre les applications de visualisation et les formats de documents en entrée de la TOE [B10.Correspondance_FormatDoc_Application]~~.

Note :

Bien que ce soit l'administrateur de l'application appelante qui configure l'application et donc ces paramètres, c'est celle-ci qui les transmet à la TOE.

5.1.5 Opérations cryptographiques

O11. 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 la DCSSI [CRYPT-STD].

5.1.6 Contrôle de l'invariance de la sémantique du document

O12. Contrôle_Invariance_Document

La TOE doit déterminer si la sémantique du document est stable.

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

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

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

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

Note :

Par construction, la TOE se charge de contrôler la stabilité du document et ne peut signer de document dit instable (cf §3.2.7).

5.1.7 Présentation du ou des documents à signer

~~O.Lancement_d'Applications_De_Présentation~~

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

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

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

O13. Présentation_Document

La TOE devra pouvoir présenter le document à signer au signataire.

Pour identifier quel type de présentation effectuer, la TOE devra gérer la correspondance entre le format pour lesquels elle autorise la signature et la présentation.

La TOE ne devra pas permettre la signature d'un document si elle ne peut afficher le contenu document en entier.

Note :

La TOE ne permet pas la contre-signature.

5.1.8 Vérification du bon fonctionnement du SCDev

O14. Vérification_Fonctionnement_SCDev

La TOE doit s'assurer que les données renvoyées par le SCDev constituent bien une signature numérique au format PKCS#1.

5.2 Objectifs de sécurité pour l'environnement

5.2.1 Machine hôte

OE1. Machine_Hôte

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

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

Les mesures suivantes devront être appliquées:

- la machine hôte est protégée contre les virus

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

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.

OE2. 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

5.2.3 Dispositif de création de signature

OE3. 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.

OE4. 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.

5.2.4 Présence du signataire

OE5. Présence_Du_Signataire

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

Note d'application

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

5.2.5 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 effectue elle-même l'affichage du document.

5.2.6 Divers

~~**OE.Contrôle_Sémantique_Document_Signé**~~

~~L'environnement de la TOE devra fournir un module capable de déterminer si la sémantique du document signé est bien invariante et de communiquer le statut de son analyse à la TOE.~~

OE6. Authenticité_Origine_Politique_Signature

Les administrateurs de ~~la TOE~~ l'application appelante (S3.Administrateur_Application_Appelante) devront s'assurer de l'authenticité de l'origine des politiques de signature avant qu'elles ne soient utilisées par la TOE.

OE7. Application_Appelante_Sûre

L'application appelante de la TOE (S2.Application_Appelante) est de confiance.

OE8. Administrateur_Développeur_sûr

Le développeur de l'application appelante de la TOE et son administrateur (S2.Application_Appelante et S3.Administrateur_Application_Appelante) sont de confiance, formés à l'utilisation de la TOE et disposent des moyens nécessaires à la réalisation de leur activité.

~~**OE.Administrateur_De_Sécurité_Sûr**~~

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

OE9. Intégrité_Services

L'environnement de la TOE devra fournir à ~~l'administrateur de sécurité~~ l'application appelante (S2.Application_Appelante) et/ou son administrateur (S3.Administrateur_Application_Appelante) les moyens de contrôler l'intégrité des services et des paramètres de la TOE.

OE10. Communication_Web

La communication entre la machine hôte sur laquelle s'exécute la TOE, et le serveur web depuis lequel sont chargées l'application appelante et la TOE, doit garantir la protection en intégrité des paramètres transmis à la TOE.

OE11. Serveur_Web

Le serveur sur lequel sont stockées la TOE et l'application appelante doit être protégé de manière à garantir l'intégrité de la TOE et de l'application appelante.

On suppose que les mesures suivantes sont appliquées:

- le serveur est protégé contre les virus
- l'accès physique au serveur est protégé
- les échanges entre le serveur 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 du serveur est restreint aux seuls administrateurs de celui-ci (remarque : l'administrateur de l'application appelante et celui du serveur peuvent être deux personnes distinctes)
- l'installation et la mise à jour de logiciels sur le serveur est sous le contrôle de l'administrateur du serveur

6. EXIGENCES DE SECURITE

6.1 Exigences fonctionnelles de sécurité de la TOE

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

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

Le composant FDP_MRU.1 utilisé dans ce chapitre a été explicitement ajouté (cf §9.1).

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 TSC.**

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~~ and signer's certificate),**
- **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 following **set of rules : none**

FDP_IFF.1.4/Document acceptance The TSF shall provide the following **additional capabilities:**

- **capability to control ~~invoke an external checker in charge of controlling~~ that the semantics of the document to be signed is invariant**
- **capability to inform the ~~signer~~ calling application when the document's semantics is not stable**
- ~~capability to request signer's explicit agreement to continue the process when the document's semantics is not stable and the signature policy allows to bypass the control.~~

FDP_IFF.1.5/Document acceptance The TSF shall explicitly authorise an information flow based on the following rules: **none.**

FDP_IFF.1.6/Document acceptance The TSF shall explicitly deny an information flow based on the following rules: **none**.

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 TSC**.**

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

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

Raffinement non éditorial:

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

Note d'application

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

FMT_MSA.3/Document's acceptance Static attribute initialisation

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

Raffinement non éditorial:

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.

Note :

The TOE always stops the signature process, when the document is considered as “instable”.

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 attribute **document's to be signed identifiers** to **the ~~signer~~ calling application**.

Note :

The TOE displays the content of the document to be signed to the user. However, the document has been sent to the TOE by the calling application, through a parameter.

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

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

- **selecting a ~~list of~~ document~~s~~ to be signed**

Refinement:

The TOE can sign only one document

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 security management functions:

- **checking the document ~~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.**~~

Refinement:

The TOE cannot sign an instable document since it presents the document to the signer and it does not presents instable document.

~~**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 security management functions:~~

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

Refinement:

The TOE cannot sign an instable document since it presents the document to the signer and it does not presents instable document.

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 [Raffiné éditorialement] 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~~ calling application**.

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 security management functions:

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

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, the Certificate Authority of the signer's certificate, the validity period time of the signer's certificate.**

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

- **each rule defined in requirement FDP_MRU.1/Signer's certificate is met, except the ones that are not explicitly referenced in the applied signature policy.**

FDP_IFF.1.3/Signer's certificate import The TSF shall enforce **none.**

FDP_IFF.1.4/Signer's certificate import The TSF shall provide the following **none.**

FDP_IFF.1.5/Signer's certificate import The TSF shall explicitly authorise an information flow based on the following rules: **none.**

FDP_IFF.1.6/Signer's certificate import The TSF shall explicitly deny an information flow based on the following rules: **none.**

FDP_MRU.1/Signer's certificate Mandatory rules

FDP_MRU.1.1/Signer's certificate The TSF shall be able to apply a set of rules in enforcing the **the signer's certificate information flow control policy**.

FDP_MRU.1.2/Signer's certificate The TSF shall be able to apply the following set of rules:

- **the "key usage" of the selected signer's certificate indicates that this certificate is usable for non repudiation purposes (Application note: bit 1 of keyUsage set)**
- **the certificate is a Qualified Certificate (Application note: information available using a QCStatement, see RFC 3739 and [EXT_TS_101_862]),**
- **the private key corresponding to public key is protected by an SSCD (Application note: information available using a QCStatement, see RFC 3739 and [EXT_TS_101_862])**
- **the certificate is issued by one of the Certificate Authorities defined by the calling application (through the signature policy)**
- **the certificate is valid at the time indicated by the calling application (through the signature policy) or by the system's time if no time is specified.**

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 **the signer's certificate information flow control policy** to restrict the ability to **select** the security attributes **signer's certificate** 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 TSC.

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 TSC: **none**.

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 following list of interpretation rules :**

- **interpretation of the DN of the signer's certificate**
- **interpretation of the Certificate Authority of the signer's certificate**
- **interpretation of the validity period time of the signer's certificate**
- **interpretation of *Key usage***
- **interpretation of the QCStatements (qualified certificate and SSCD private key protection)**

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 security 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 numeric signature (once generated)**
- **operations:**
  - **transfert to the SCDev**

FDP_IFF.1/Signature generation Simple security attributes

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

- **subjects: the signer (applied signature policy, signer's certificate), ~~signer's explicit agreement to sign the present non invariant document~~ (see FDP_IFF.1.4/Signature generation, the SCDev)**
- **information: the data to be signed formatted (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:

- **each rule defined in requirements FDP_MRU.1/Signature attributes is met, except the ones that are not explicitly referenced in the applied signature policy.**

FDP_IFF.1.3/Signature generation The TSF shall enforce the following **:** **none**

FDP_IFF.1.4/Signature generation The TSF shall provide the following **additional capabilities:**

- **capability to communicate the signature attributes to the signer before the signature generation**
- **capability to ~~launch the viewer corresponding to the document's format~~ display the document according to *document format/viewer association table***
- **capability to activate the signing key corresponding to the selected signer's certificate.**
- **transfer the formatted data to be signed to the SCDev and receive the signature**

FDP_IFF.1.5/Signature generation The TSF shall explicitly authorise an information flow based on the following rules: **none**.

FDP_IFF.1.6/Signature generation The TSF shall explicitly deny an information flow based on the following rules: **none**.

FDP_MRU.1/Signature attributes Mandatory rules

FDP_MRU.1.1/Signature attributes The TSF shall be able to apply a set of rules in enforcing **the signature generation information flow control policy**.

FDP_MRU.1.2/Signature attributes The TSF shall be able to apply the following set of rules:

- **~~if the signature policy requires the inclusion of the signature attribute "signature policy identifier", then its~~ The value of "signature policy identifier" 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.**

Raffinement non éditorial :

La politique de signature ne restreint jamais les valeurs que peuvent prendre « commitment type » et « claimed role ».

En effet, l'application spécifiant elle-même et au même instant la politique de signature, le rôle et le type d'engagement, il est inutile que la politique de signature restreigne les valeurs possibles pour ces deux paramètres.

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 TSC**.**

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

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 TSC: **the user have to check a *checkbox* to explicitly give his 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 generated numeric signature**
  - **the signature attributes: ~~document~~ data (to be signed)'s hash, ~~reference to~~ the signer's certificate**
- **operations:**
  - **export to the signer.**

FDP_IFF.1/Electronic signature export Simple security attributes

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

- **subjects:**
  - **the signer**
  - **the SCDev (the status of signature generation process)**
- **information:**
  - **the electronic signature (the generated numeric signature, the signed ~~document~~ data's hash, ~~the reference to~~ the signer's certificate, the reference of the applied signature policy).**

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 **following additional set of rules :**

- **Export of the electronic signature to the signer is allowed if the numeric signature is in a PKCS#1 format.**

FDP_IFF.1.4/Electronic signature export The TSF shall provide the following **following additional capability :**

- **Format the signature to XAdES (version 1.1.1 or 1.2.2) format.**

FDP_IFF.1.5/Electronic signature export The TSF shall explicitly authorise an information flow based on the following rules: **none.**

FDP_IFF.1.6/Electronic signature export The TSF shall explicitly deny an information flow based on the following rules: **none.**

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 TSC**.**

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 TSC, 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 TSC: **none.**

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 security management functions:

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

6.1.6 Opérations 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

- **SHA-1**
- **SHA-256**

~~and cryptographic key sizes [assignment: *cryptographic key sizes*]~~

that meet the following: [**CRYPT-STD**], **[FIPS 180-2]**.

Refinement:

cryptographic key sizes is not applicable in the context of this hash function.

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**~~ **the calling application**

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 identify itself before allowing any other TSF-mediated actions on behalf of that user.

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**~~ **nobody.**

Note :

Cette table est figée dans la TOE. Elle possède deux entrées : la première pour le texte brut, la seconde pour le HTML.

FMT_SMF.1/Management of the document/format association table Specification of management functions

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

- **allow ~~the administrator of the TOE~~ nobody to manage 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 **define** the **signature policies to the ~~security administrator~~ the calling application of the TOE.**

Note :

La politique de signature est transmise par l'application appelante à la TOE lors de l'appel. Elle est cependant définie par l'administrateur de l'application appelante.

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 security management functions: **define.**

6.2 Exigences de sécurité d'assurance pour la TOE

Le niveau des exigences de sécurité d'assurance est EAL3. L'EAL a été augmentée avec ADV_IMP.1 (pour FCS seulement), ADV_LLD.1 (pour FCS seulement), ALC_FLR.3, ALC_TAT.1 (pour FCS seulement) et AVA_VLA.2.

7. SPECIFICATION GLOBALES DE LA CIBLE D'EVALUATION

Cette section décrit les fonctions de sécurité implémentée par la TOE pour satisfaire les exigences et les objectifs.

7.1 Fonction de sécurité de la TOE

7.1.1 F. Signature

Cette fonction signe un document.

Elle prend en entrée les paramètres suivants :

- De la part de l'application appelante, au travers de l'interface d'appel :
  - le document à signer, sous forme de données brutes encodées en base64
  - la page web vers laquelle le signataire sera dirigé en cas d'erreur
  - la version de la signature XAdES à générer
  - l'algorithme de hachage (SHA-1 ou SHA-256)
- De la part de F.Contrôle_Invariance_Sémantique :
  - Le statut du contrôle de stabilité sémantique
- De la part de F.Applique_Politique_Signature :
  - référence de la politique de signature
  - le type d'engagement
  - rôle du signataire
  - lieu de signature (si spécifié)
- Le consentement explicite de signature du document
- De la part de F.Sélection_Certificat :
  - Le certificat à utiliser pour la signature du document

La fonction F.Signature demande la signature d'un document lorsqu'elle a obtenu le consentement de l'utilisateur. Pour cela :

- Elle formate les données à signer en fonction de la version (1.1.1 ou 1.2.2) de la signature XAdES à générer. Elle calcule ensuite le condensé de ces données suivant l'algorithme SHA-1 ou SHA-256, puis formate ce condensé (en ajoutant l'OID de l'algorithme de hachage utilisé).
- Elle retourne le document signé

La signature du document comprend entre autre les informations suivantes :

- La signature numérique générée par le SCDev à partir du condensé du document
- Le condensé du document signé
- Le certificat du signataire
- Une référence à la politique de signature appliquée

En cas d'erreur, l'utilisateur est redirigé vers la page web d'échec.

A tout moment l'utilisateur peut interrompre le processus de signature, avant que les données ne soient envoyées au SCDev.

7.1.2 F.Contrôle_Invariance_Sémantique

La TOE contrôle l'invariance de la sémantique du document.

- Si les données sont à interprétées en texte brut, la sémantique est considérée stable,
- Si les données sont à interprétées en HTML, la TOE vérifie que le contenu du document respecte le format HTML défini dans le guide d'intégration [IGS].

Si la sémantique du document est instable, la fonction retourne une erreur qui arrêtera immédiatement le processus de signature.

7.1.3 F.Sélection_Certificat

Cette fonction demande au signataire de sélectionner un certificat.

Les certificats proposés au signataire répondent à la politique de signature, c'est-à-dire que la liste des certificats proposés a été filtrée suivant la politique de signature.

7.1.4 F.Présentation_Document

Elle présente le contenu du document au signataire : soit à l'intérieur d'un encadré (« textbox ») lorsque le document est au format texte brut, soit sous forme graphique lorsque le document est au format HTML (seules sont reconnues les balises HTML définies dans le guide d'intégration [IGS]).

Elle prend en entrée :

- Le contenu du document à signer,
- La manière dont les données doivent être interprétées par la TOE (soit HTML soit texte brut).

7.1.5 F.Administration

Cette fonction permet à l'application appelante de spécifier :

- La politique de signature (dont les éléments sont rappelés au paragraphe 7.1.6)
- La manière dont les données doivent être interprétées par la TOE (soit HTML soit texte brut).

7.1.6 F.Applique_Politique_Signature

Une politique de signature est définie par les données suivantes :

- la liste des ACs autorisées,
- la clé publique du certificat à afficher,
- une référence de la politique de signature qui sera incluse dans les données à signer,
- une date de filtrage : les certificats antérieurs à cette date ne sont pas pris en compte,
- le type d'engagement (inclus dans les données à signer),
- rôle du signataire (inclus dans les données à signer),
- lieu de signature (inclus dans les données à signer),
- Le certificat est utilisable ou non pour des applications de non répudiation (bit 1 du paramètre KeyUsage),
- Le certificat est ou non qualifié
- La clé privée est ou non protégée par un SSCD

Si certains paramètres n'ont pas de valeurs définies par l'application appelante, alors les valeurs par défauts suivantes sont utilisées :

- liste des ACs autorisées : toutes
- clé publique du certificat : aucune
- date de filtrage : la date du jour sur le poste client est utilisée pour le filtrage
- le type d'engagement : aucun
- rôle du signataire : aucun
- lieu de signature : aucun
- ne pas requérir la non-répudiation : 0
- certificat non qualifié : 0
- clé privée non protégée par SSCD : 0

Cette fonction applique la politique de signature :

- Elle filtre les certificats disponibles pour le signataire en fonction des paramètres suivant :
  - les ACs autorisées,
  - la clé publique du certificat à afficher (dans ce cas-là un seul certificat est autorisé),
  - une date de filtrage : les certificats antérieurs à cette date ne sont pas pris en compte,
  - requiert ou non la non-répudiation,
  - le certificat est un certificat qualifié ou non [EXT_TS_101_862]
  - La clé privée est protégée par SSCD ou non [EXT_TS_101_862]
- Et elle insère dans les attributs de signature les données de la politique de signature marquées comme telle. Ces données sont :
  - Une référence de la politique de signature
  - Le type d'engagement
  - Le rôle du signataire
  - La date de la signature (date de la machine hôte)
  - Le lieu de signature

7.1.7 F.Transfert_vers_SCDev

Cette fonction communique avec le SCDev :

- Elle demande au SCDev les certificats accessibles à l'utilisateur
- Et elle demande la signature au format PKCS#1 du condensé formaté en utilisant le certificat sélectionné par le signataire (au travers d'une référence à la clé privée de l'utilisateur). Après réception de la signature, elle vérifie que cette dernière est bien au format PKCS#1. Si ce n'est pas le cas elle renvoi un code d'erreur.

7.1.8 F.Présentation_attributs

Cette fonction présente les attributs de signature au signataire. Les attributs de signature sont inclus dans la signature et sont les suivants :

- référence de la politique de signature,
- le type d'engagement,
- rôle du signataire (si spécifié),

- référence au certificat de signature (sélectionné par le signataire) : CN du certificat, numéro de série du certificat, CN de l'autorité de certification, date d'émission du certificat,
- date de signature (date de la machine hôte),
- lieu de signature (si spécifié).

7.2 Mesures d'assurance pour la cible d'évaluation

Les mesures d'assurance suivantes sont nécessaires pour le niveau d'évaluation EAL3 augmenté demandé au paragraphe 6.2 :

- Des procédures et outils de gestion de configuration
- Des procédures pour la sécurité de développement
- Des documents de développement et des outils de développement
- Une documentation de test
- Une analyse de vulnérabilité
- Une procédure de livraison
- Des procédures de correction d'anomalies
- Une procédure d'installation et de démarrage
- Un guide d'utilisation pour le signataire
- Un guide pour le développement d'applications externes

7.2.1 Développement

7.2.1.1 Documents de développement et des outils de développement

Les documents de développement décrivent les fonctions de sécurité de la TOE suivant plusieurs niveaux de description.

Le premier niveau décrit les interfaces externes de la TOE (visibles pour l'utilisateur), et le comportement des fonctions de sécurité (paramètres d'entrées, réponses en sortie, messages d'erreur, …).

Le second niveau décrit la TOE en termes de sous-systèmes, précisant leurs comportements et leurs interactions.

Le troisième et le dernier niveau de description ne s'appliquent qu'à la fonction cryptographique spécifiée au travers de l'exigence *FCS_COP.1/Hash function*, à savoir, le calcul de condensats.

Un document de correspondance de la TOE permet de liés ces différents niveaux de description.

Les documents fournis pour répondre à ces mesures sont :

- Spécifications fonctionnelles,
- Architecture du produit,
- Architecture détaillée de la fonction de hachage,
- Code source de la fonction de hachage,
- Document de correspondance

Ces mesures d'assurance couvrent les exigences suivantes :

- ADV_FSP.1
- ADV_HLD.2
- ADV_LLD.1

- ADV_IMP.1
- ADV_RCR.1

7.2.2 Support au développement et livraison

7.2.2.1 Procédures de développement et outils de gestion de configuration

Un système automatique de gestion de configuration permet de gérer et contrôler l'accès au code source du produit.

Il permet d'identifier de manière unique chaque composant du produit et d'affecter un identifiant et numéro de version unique au produit.

Les procédures de développement décrivent comment utiliser le système de gestion de configuration.

Ces procédures décrivent aussi les procédures à respecter pour assurer la sécurité de l'environnement de développement, l'intégrité du code source et la confidentialité des documents de développement.

Le document fourni pour répondre à ces mesures est :

- Procédures de développement

Ces mesures d'assurance couvrent les exigences suivantes :

- ACM_CAP.3
- ACM_SCP.1
- ALC_DVS.1
- ALC_TAT.1

7.2.2.2 Procédures de correction d'anomalies

Des procédures de corrections d'anomalies sont mises en place pour assurer la réception des remontées d'anomalies, la gestion de ces anomalies, leur correction, puis la diffusion des correctifs associés, une fois ces anomalies résolues.

Le document fourni pour répondre à ces mesures est :

- Correction d'anomalies

Cette mesure d'assurance couvre l'exigence suivante :

- ALC_FLR.3

7.2.2.3 Procédure de livraison

Une procédure de livraison décrit comment le produit est livré afin de maintenir sa sécurité pour détecter toute modification non autorisée du produit durant la livraison.

Le document fourni pour répondre à ces mesures est :

- Procédure de livraison

Cette mesure d'assurance couvre l'exigence suivante :

- ADO_DEL.1

7.2.3 Tests et analyse de vulnérabilité

7.2.3.1 Documents de test

Les documents de test sont composés du plan de test, des résultats attendus et des résultats obtenus. Un document décrit la couverture des fonctions de sécurité par les tests réalisés.

Le document fourni pour répondre à ces mesures est :

- Dossier de test

Ces mesures d'assurance couvrent les exigences suivantes :

- ATE_COV.2
- ATE_DPT.1
- ATE_FUN.1
- ATE_IND.2

7.2.3.2 Analyse de vulnérabilité

Un document décrit l'analyse de vulnérabilité menée sur le produit pour identifier les vulnérabilités potentielles du produit.

La TOE ne possédant pas de mécanisme permutationnel ou probabilistique, le composant AVA_SOF.1 ne s'applique pas.

Le document fourni pour répondre à ces mesures est :

- Dossier d'analyse de vulnérabilité

Ces mesures d'assurance couvrent l'exigence suivante :

- AVA_VLA.2

7.2.4 Guides

7.2.4.1 Procédure d'installation et de démarrage

Une procédure permet d'assurer une installation et un démarrage du produit garantissant une configuration sûre du produit.

Le document fourni pour répondre à ces mesures est :

- Procédure d'installation

Cette mesure d'assurance couvre l'exigence suivante :

- ADO_IGS.1

7.2.4.2 Guide pour le développement d'applications externes

Un guide s'adressant aux développeurs d'applications écrit la manière d'utiliser les fonctions de sécurité du produit et leurs interfaces.

Ce guide stipule aussi que le guide utilisateur doit être accessible en ligne pour les signataires (cf. §7.2.4.3).

Le document fourni pour répondre à ces mesures est :

- Guide de développement d'applications

Cette mesure d'assurance couvre l'exigence suivante :

- AGD_ADM.1

7.2.4.3 Guide pour le signataire

Un guide d'utilisation s'adressant aux signataires est disponible. Cependant, de part la nature même de la TOE, ce guide n'est disponible qu'en ligne. Il doit être intégré à l'application appelante.

Le document fourni pour répondre à ces mesures est :

- Guide d'utilisation

Cette mesure d'assurance couvre l'exigence suivante :

- AGD_USR.1

7.2.5 Couverture des mesures d'assurance

Composant d'assurance	Mesure d'assurance
ACM_CAP.3	§7.2.2.1
ACM_SCP.1	§7.2.2.1
ADO_DEL.1	§7.2.2.3
ADO_IGS.1	§7.2.4.1
ADV_FSP.1	§7.2.1.1
ADV_HLD.2	§7.2.1.1
ADV_LLD.1	§7.2.1.1
ADV_IMP.1	§7.2.1.1
ADV_RCR.1	§7.2.1.1
AGD_ADM.1	§7.2.4.2
AGD_USR.1	§7.2.4.3
ALC_DVS.1	§7.2.2.1
ALC_TAT.1	§7.2.2.1
ALC_FLR.3	§7.2.2.2
ATE_COV.2	§7.2.3.1
ATE_DPT.1	§7.2.3.1
ATE_FUN.1	§7.2.3.1
ATE_IND.2	§7.2.3.1
AVA_MSU.1	§7.2.4.1 §7.2.4.2 §7.2.4.3
AVA_SOF.1	-
AVA_VLA.1	§7.2.3.2

Les mesures d'assurance définies dans ce paragraphe couvrent l'ensemble des composants d'assurance.

8. CONFORMITE AU PROFIL DE PROTECTION

Ce chapitre fournit les déclarations de conformité à un profil de protection.

8.1 Référence du Profil de protection

La cible de sécurité est conforme au Profil de protection « Application de création de signature » [EXT_DCSSI_PP].

8.2 Modifications apportées par rapport au Profil de protection

Les modifications apportées par rapport au profil de protection sont été indiquées dans la cible de sécurité par bleu souligné pour les ajouts et ~~orange barré~~ pour les suppressions.

Les spécificités de la présente cible de sécurité vis-à-vis du profil de protection sont énoncées ci-après.

Les modifications sont présentées par thème (politique de signature, affichage, contrôle de sémantique, …). A la fin un tableau récapitule l'ensemble des modifications par catégorie (biens, sujets, hypothèses, menaces,…).

8.2.1 Les sujets

Compte-tenu de la TOE, cette dernière se doit de prendre en compte plusieurs rôles et pas seulement celui d'administrateur de sécurité de la TOE.

Ce dernier rôle a été supprimé pour être remplacé par les trois suivants :

- Le développeur d'une application appelante (page web) : il développe la page web qui appellera la TOE, en respectant le guide de développement pour connaître la manière de transmettre les paramètres d'entrée à la TOE et recevoir la signature et les code d'erreur que renvoie celle-ci ;
- L'administrateur de l'application appelante : il gère les politiques de signature utilisables par l'application appelante et donc par la TOE (puisque la politique lui est transmise en paramètre d'entrée) ;
- Et enfin, l'application appelante (page web) elle-même qui joue le rôle d'administrateur de la TOE, puisque c'est elle qui transmet la politique de signature à appliquer. Elle transmet aussi le contenu du document à signer.

Catégorie	Nom de l'élément	Modification apportée	Commentaires
Sujet	S.Administrateur_de_securité	Suppression du sujet	L'administrateur de sécurité de la TOE a été scindé en S2,S3 et S4
Sujet	S2.Application_Appelante	Ajout du sujet	-
Sujet	S3.Administrateur_Application_Appelante	Ajout du sujet	-
Sujet	S4.Developpeur_Application_Appelante	Ajout du sujet	-

Puisque des hypothèses et objectifs de sécurité sur l'environnement étaient attachés au sujet « administrateur de sécurité », ils ont été supprimés pour ce dernier et ajoutés pour les nouveaux sujets :

Catégorie	Nom de l'élément	Modification apportée	Commentaires
Hypothèse	H.Administrateur_De_Sécurité_Sûr	Suppression de l'hypothèse	Scindée en H6 et H7, afin de préciser les rôles de l'application appelante et de l'administrateur
Hypothèse	H6.Application_Appelante_Sûre	Ajout de l'hypothèse	-
Hypothèse	H7.Développeur_Administrateur_sûr	Ajout de l'hypothèse	-
Objectif	OE. Administrateur_De_Sécurité_Sûr	Suppression de l'objectif	-
Objectif	OE7.Application_Appelante_Sûre	Ajout de l'objectif	-
Objectif	OE8.Administrateur_Développeur_sûr	Ajout de l'objectif	-

Et les précisions suivantes ont dues être apportées :

Catégorie	Nom de l'élément	Modification apportée	Commentaires
Hypothèse	H8.Intégrité_Services	Modification au niveau des mots *administrateur de sécurité*	-
Objectif	OE9.Intégrité_Services	Modification au niveau des mots *administrateur de sécurité*	-
Exigence fonctionnelle de sécurité	FMT_SMR.1 Security roles	Raffinement	L'administrateur de la TOE est changé en l'application appelante

8.2.2 La présentation de document

Le profil de protection demande que la TOE puisse faire appel à un module externe pour afficher le contenu du document et le cas échéant toute signature déjà apposée.

Cet affichage est possible grâce à :

- la possibilité par la TOE d'appeler un module externe,
- la présence d'un ou plusieurs modules externes (applications de visualisation),
- et un tableau de correspondance entre le format du document à visualiser et l'application de visualisation de ce document, tableau présent dans la TOE.

La TOE décrite dans cette cible de sécurité effectue elle-même l'affichage du document à signer. Les types de documents reconnus par la TOE sont : le texte brut et le HTML. Pour ce dernier type, seuls certaines balises HTML sont reconnues (elles sont décrites dans le guide d'intégration [IGS]).

Si le document ne peut être affiché, la TOE arrête le processus de signature.

Enfin, la TOE ne permet pas la contre-signature.

Il est donc :

- nécessaire d'apporter des précisions dans les éléments suivants :

Catégorie	Nom de l'élément	Modification apportée	Commentaires
Bien	B10.Correspondance_FormatDoc_Application	Précisions	La présentation est effectuée par la TOE et le tableau de correspondance est figé
OSP	P5.Possibilité_De_Présenter_Le_Document	Précision sur la présentation du document	-
Exigence fonctionnelle de sécurité	FDP_IFF.1/Signature generation	Raffinement	La TOE effectue elle-même l'affichage
Exigence fonctionnelle de sécurité	FMT_SMF.1/Management of the document/format association table	Raffinement	Personne ne peut modifier la table, puisqu'elle est figée dans la TOE
Exigence fonctionnelle de sécurité	FMT_MTD.1/Document format/viewer association table	Raffinement	La table est figée dans la TOE, c'est pourquoi personne ne peut la modifier

- nécessaire d'ajouter les éléments suivants :

Catégorie	Nom de l'élément	Modification apportée	Commentaires
Objectif	O13.Présentation_Document	Ajout	La TOE présente elle-même le contenu du document à signer

- et inutile de conserver par rapport au profil de protection les éléments suivants :

Catégorie	Nom de l'élément	Modification apportée	Commentaires
Hypothèse	H.Présentation_Du_Document	Suppression de l'hypothèse car la présentation est effectuée par la TOE	-
Hypothèse	H.Présentation_Signatures_Existantes	Suppression de l'hypothèse car la présentation est effectuée par la TOE	Toutefois, il faut noter que la TOE ne permet pas la contre-signature
Objectif	O.Lancement_d'Applications_De_Présentation	Suppression	La TOE présente elle-même le contenu du document à signer
Objectif	OE.Présentation_Document	Suppression	La TOE présente elle-même le contenu du document à signer

8.2.3 Le contrôle d'invariance sémantique

Le profil de protection demande que la TOE puisse faire appel à un module externe pour vérifier le l'invariance sémantique du document.

Ce contrôle est possible grâce à :

- la possibilité par la TOE d'appeler un module externe,
- la présence d'un module externe.

Dans le cas où le contrôle révèle que le document est instable (donc non invariant), la TOE doit :

- en informer le signataire,
- et, si la politique de signature l'autorise, lui demander son consentement à signer un document instable.

La TOE décrite dans cette cible de sécurité effectue elle-même le contrôle de sémantique du document à signer, lorsque celui-ci est au format HTML (puisque le format texte brut est invariant par nature). Pour cela, elle s'appuie sur les balises HTML qu'elle reconnaît comme étant invariantes.

Il n'est donc plus utile de faire appel à un module externe.

De plus, lorsqu'une balise est jugée instable, elle ne pourra être affichée par la TOE. Il n'est donc pas nécessaire de demander au signataire s'il souhaite signer un document instable, puisque le profil de protection requiert que le processus de signature soit arrêté lorsque le document ne peut être affiché.

Il est donc :

- nécessaire d'apporter des précisions dans les éléments suivants :

Catégorie	Nom de l'élément	Modification apportée	Commentaires
OSP	P4.Sémantique_Document_Invariante	Précision et suppression de texte	La TOE effectue le contrôle d'invariance
Objectif	O12.Contrôle_Invariance_Document	Précision sur le contrôle d'invariance et suppression de texte	Ce contrôle est effectué par la TOE
Exigence fonctionnelle de sécurité	FDP_IFF.1/Document acceptance	Raffinement	Le contrôle d'invariance est effectué par la TOE
Exigence fonctionnelle de sécurité	FDP_IFF.1/Document acceptance	Suppression de la demande de signer un document instable	En effet, si le document est instable, la TOE ne peut l'afficher et donc le processus de signature est arrêté
Exigence fonctionnelle de sécurité	FDP_ITC.1/Document acceptance Import of user data without security attributes	Raffinement	Le contrôle d'invariance est effectué par la TOE
Exigence fonctionnelle de sécurité	FMT_MSA.3/Document's acceptance	Raffinement	La TOE arrête le processus de signature si le document est instable
Exigence fonctionnelle de sécurité	FMT_SMF.1/Getting document's semantics invariance status	Raffinement	Le contrôle d'invariance est effectué par la TOE

- et inutile de conserver par rapport au profil de protection les éléments suivants :

Catégorie	Nom de l'élément	Modification apportée	Commentaires
Hypothèse	H.Contrôle_Invariance_Sémantique_Document	Suppression de l'hypothèse	Puisque le contrôle est fait par la TOE
Objectif	OE.Contrôle_Sémantique_Document_Signé	Suppression de l'objectif	Le contrôle est effectué par la TOE
Exigence fonctionnelle de sécurité	FMT_MSA.1/Signer agreement to sign an instable document	Suppression de l'exigence	En effet, la signature sera toujours refusée dans le cas d'un document instable
Exigence fonctionnelle de sécurité	FMT_SMF.1/Getting signer agreement to sign an instable document	Suppression de l'exigence	En effet, la signature sera toujours refusée dans le cas d'un document instable
Exigence fonctionnelle de sécurité	FDP_IFF.1/Signature generation Simple security attributes	Suppression de l'import de l'attribut « signer's explicit agreement to sign the present non invariant document »	-

8.2.4 Signature au format XAdES

La signature que retourne la TOE est au format XAdES. Pour cela les ajouts / raffinements suivants ont été effectués :

Catégorie	Nom de l'élément	Modification apportée	Commentaires
Bien	B3.Données_à_signer_formatées	Précision sur le format de la signature	Signature XAdES
Bien	B6.Signature_électronique	Précision sur le contenu de la signature	Signature XAdES
OSP	P12.Export_Signature_Electronique	Précision sur le format de la signature	Signature XAdES
Objectif	O9.Export_Signature_Electronique	Précision sur le format de la signature	Signature XAdES
Exigence fonctionnelle de sécurité	FDP_IFF.1/Electornic signature export	Raffinement	Ajout de la capacité de formater la signature au format XAdES

8.2.5 Vérification du format PKCS#1

La TOE vérifie que le format de la signature renvoyée par le SCDev est bien au format PKCS#1. Pour cela, les éléments suivants ont été ajoutés ou raffinés :

Catégorie	Nom de l'élément	Modification apportée	Commentaires
OSP	P14.Vérification_Fonctionnement_SCDev	Ajout la politique organisationnelle	-

Objectif	O14.Vérification_Fonctionnement_SCDev	Ajout suite à P14	-
Exigence fonctionnelle de sécurité	FDP_IFF.1/Electornic signature export	Raffinement	Ajout de la capacité à vérifier que la signature générée est au format PKCS#1

8.2.6 Politique de signature

Le profil demande à ce que l'administrateur de sécurité puisse effectuer des opérations sur les politiques de signature applicables.

Dans le cas de la présente TOE, la politique de signature est définie par le passage de paramètres effectué par l'application appelante. Les modifications suivantes ont été apportées :

Catégorie	Nom de l'élément	Modification apportée	Commentaires
Sujet	S1.Signataire	Précision sur la politique de signature	Elle est définie par l'application appelante
OSP	P13.Administration	Précision sur la gestion des politiques de signature	la politique de signature est définie par l'application appelante
Objectif	O10.Administration	Précision sur la gestion des politiques de signature	C'est l'application appelante qui peut définir la politique de signature au travers d'un paramètre d'entrée
Objectif	OE6.Authenticité_Origine_Politique_Signature	Modification au niveau du mot *TOE*	-
Exigence fonctionnelle de sécurité	FMT_MSA.1/Signature attributes	Précision sur la gestion des arributs de signature	C'est l'application appelante qui peut définir les attributs de signature au travers d'un paramètre d'entrée
Exigence fonctionnelle de sécurité	FMT_MTD.1/Management of the signature policies	Assignement	Operation possible : "define"
Exigence fonctionnelle de sécurité	FMT_MTD.1/Management of the signature policies	Raffinement	C'est l'application appelante qui peut définir la politique de signature
Exigence fonctionnelle de sécurité	FMT_SMF.1/Management of the signature policies	Assignement	Operation possible : "define"
Exigence fonctionnelle de sécurité	FDP_MRU.1/Signature attributes Mandatory rules	Modification	La présence de la référence de la politique de signature est obligatoire

8.2.7 Signature d'un seul document

La TOE ne permet de signer qu'un document à la fois. Bien que explicitement autorisé par le profil de protection sans avoir à modifier ni les OSP, ni les objectifs, ni les exigences fonctionnelles, un raffinement a cependant été apporté afin de rendre la capacité de signer un seul document à la fois plus explicite :

Catégorie	Nom de l'élément	Modification apportée	Commentaires
Bien	B.Ensemble_Des_Documents_A_Signer	Renommé en B1.Document_à_signer et modifié	Un seul document peut être signé par la TOE
Sujet	S1.Signataire	Précision sur le fait qu'un seul document peut être signé par la TOE	-
OSP	P8.Signature_De_Document	Modification de l'intitulé (anciennement P.Signature_De_ Plusieurs_Document) Précision sur le fait qu'un seul document peut être signé par la TOE	-
Objectif	O5.Document_A_Signer	Modification de l'intitulé (anciennement O. Ensemble_De_ Documents_A_Signer) Modification du contenu de l'objectif	Un seul document peut être signé par la TOE
Exigence fonctionnelle de sécurité	FMT_SMF.1/Selection of a list of documents	Raffinement	Un seul document peut être signé par la TOE

8.2.8 Contexte d'utilisation

La TOE est stockée sur un serveur d'application web pour être ensuite téléchargée par l'utilisateur final avant son utilisation.

Ceci nécessite l'ajout d'hypothèses et d'objectifs de sécurité sur l'environnement concernant le serveur d'application web et le canal de communication entre le serveur et le navigateur de l'utilisateur.

Ainsi ont été rajoutés :

Catégorie	Nom de l'élément	Modification apportée	Commentaires
Hypothèse	H10.Communication_Web	Ajout de l'hypothèse	Les informations doivent transmises de manière sûre
Hypothèse	H11.Serveur_Web	Ajout de l'hypothèse	Le serveur d'application web doit être protégé
Objectif	OE10.Communication_Web	Ajout de l'objectif sur	Les informations

		l'environnement	doivent transmises de manière sûre
Objectif	OE11.Serveur_Web	Ajout de l'objectif sur l'environnement	Le serveur d'application web doit être protégé

8.2.9 Autres assignements

Les *assignements* suivants demandés par le profil de protection, et ne faisant pas partie d'un thème précis, ont été effectués :

Catégorie	Nom de l'élément	Modification apportée	Commentaires
Exigence fonctionnelle de sécurité	FDP_IFF.1/Document acceptance	Assignement	Autres attribut du signataire
Exigence fonctionnelle de sécurité	FDP_IFF.1/Signer's certificate import	Assignement	Autres attributs du certificat du signataire
Exigence fonctionnelle de sécurité	FDP_MRU.1/Signer's certificate	Assignement	Autres règles concernant les champs du certificat
Exigence fonctionnelle de sécurité	FPT_TDC.1/Signer's certificate	Assignement	Règles d'interprétation d'un certificat
Exigence fonctionnelle de sécurité	FDP_IFF.1/Signature generation	Assignements	Autres attributs de signature
Exigence fonctionnelle de sécurité	FDP_ITC.1/Explicit signer agreement	Assignement	Description de ce que le signataire doit effectuer pour donner son consentement explicite à signer un document
Exigence fonctionnelle de sécurité	FCS_COP.1/Hash function	Assignement	Algorithme de hachage et standard FIPS 180-2

8.2.10 Autres raffinements

Concernant les autres *raffinements* non encore cités, le présent tableau résume les différences par rapport au profil de protection :

Catégorie	Nom de l'élément	Modification apportée	Commentaires
Objectif	O7.Validité_Du_Certificat	Raffinement	Précision sur la référence de temps utilisée par la TOE
Exigence fonctionnelle de sécurité	FDP_IFF.1/Signature generation	Raffinement	a) Il faut aussi que les règles concernant le certificat et décrite par FDP_MRU.1/Signer's certificate soient respectées

			b) Et que la TOE ait la capacité de transférer les données à signées formatées au SCDev, et de recevoir cette signature de la part du SCDev
Exigence fonctionnelle de sécurité	FMT_MSA.1/Selected documents	Raffinement	C'est l'application appelante qui transmet à la TOE le contenu du document à signer
Exigence fonctionnelle de sécurité	FDP_IFC.1/Electronic signature export	Raffinement	Précision sur la nature des attributs de signature afin de correspondre à l'objectif de sécurité O5
Exigence fonctionnelle de sécurité	FDP_IFF.1/Electronic signature export	Raffinement	Précision sur la nature des attributs de signature afin de correspondre à l'objectif de sécurité O5
Exigence fonctionnelle de sécurité	FDP_MRU.1/Signature attributes Mandatory rules	Raffinement (non editorial)	Précision sur le fait qu'il est inutile à la TOE de vérifier la conformité des valeurs prises par le type d'engagement et le rôle du signataire

8.2.11 Autres biens

Concernant les autres biens non encore cités, le présent tableau résume les différences par rapport au profil de protection :

Catégorie	Nom de l'élément	Modification apportée	Commentaires
Bien	B2.Données_à_signer	Précisions sur le type de données à signer, et les attributs de signature (certains ne sont utilisés que lorsqu'ils sont spécifiés par l'application appelante)	-
Bien	B5. Condensé_formaté	Ajout de précisions	-
Bien	B7.Politique_de_signature	Précision sur les éléments constituant la politique de signature	-

8.3 Récapitulatif des modifications

Ce paragraphe reprend les tableaux présentés précédemment et regroupe les informations par catégorie d'élément :

Catégorie	Nom de l'élément	Modification apportée	Commentaires
Bien	B.Ensemble_Des_Documents_A_Signer	Renommé en B1.Document_à_signer et modifié	Un seul document peut être signé par la TOE
Bien	B2.Données_à_signer	Précisions sur le type de données à signer, et les attributs de signature (certains ne sont utilisés que lorsqu'ils sont spécifiés par l'application appelante)	-
Bien	B3.Données_à_signer_formatées	Précision sur le format de la signature	Signature XAdES
Bien	B5. Condensé_formaté	Ajout de précisions	-
Bien	B6.Signature_électronique	Précision sur le contenu de la signature	Signature XAdES
Bien	B7.Politique_de_signature	Précision sur les éléments constituant la politique de signature	-
Bien	B10.Correspondance_FormatDoc_Application	Précisions	La présentation est effectuée par la TOE et le tableau de correspondance est figé
Sujet	S1.Signataire	Précision sur la politique de signature	Elle est définie par l'application appelante
Sujet	S1.Signataire	Précision sur le fait qu'un seul document peut être signé par la TOE	-
Sujet	S.Administrateur_de_securité	Suppression du sujet	L'administrateur de sécurité de la TOE a été scindé en S2,S3 et S4
Sujet	S2.Application_Appelante	Ajout du sujet	-
Sujet	S3.Administrateur_Application_Appelante	Ajout du sujet	-
Sujet	S4.Developpeur_Application_Appelante	Ajout du sujet	-
Hypothèse	H.Présentation_Du_Document	Suppression de l'hypothèse car la présentation est effectuée par la TOE	
Hypothèse	H.Présentation_Signatures_Existantes	Suppression de l'hypothèse car la présentation est effectuée par la TOE	Toutefois, il faut noter que la TOE ne permet pas la contre-signature
Hypothèse	H.Contrôle_Invariance_Sémantique_Document	Suppression de l'hypothèse	Puisque le contrôle est fait par la TOE
Hypothèse	H6.Application_Appelante_Sûre	Ajout de l'hypothèse	-
Hypothèse	H7.Développeur_Administrateur_sûr	Ajout de l'hypothèse	-
Hypothèse	H.Administrateur_De_Sécurité_Sûr	Suppression de l'hypothèse	Scindée en H6 et H7, afin de préciser les rôles de l'application appelante et de l'administrateur
Hypothèse	H8.Intégrité_Services	Modification au niveau des mots *administrateur de*	-

		sécurité	
Hypothèse	H10.Communication_Web	Ajout de l'hypothèse	Les informations doivent transmises de manière sûre
Hypothèse	H11.Serveur_Web	Ajout de l'hypothèse	Le serveur d'application web doit être protégé
OSP	P4.Sémantique_Document_Invariante	Précision	La TOE effectue le contrôle d'invriance
OSP	P5.Possibilité_De_Présenter_Le_Document	Précision sur la présentation du document	-
OSP	P8.Signature_De_Document	Modification de l'intitulé (anciennement P.Signature_De_ Plusieurs_Document) Précision sur le fait qu'un seul document peut être signé par la TOE	-
OSP	P12.Export_Signature_Electronique	Précision sur le format de la signature	Signature XAdES
OSP	P13.Administration	Précision sur la gestion des politiques de signature	la politique de signature est définie par l'application appelante
OSP	P14.Vérification_Fonctionnement_SCDev	Ajout la politique organisationnelle	-
Objectif	O5.Document_A_Signer	Modification de l'intitulé (anciennement O. Ensemble_De_ Documents_A_Signer) Modification du contenu de l'objectif	Un seul document peut être signé par la TOE
Objectif	O7.Validité_Du_Certificat	Raffinement	Précision sur la référence de temps utilisée par la TOE
Objectif	O9.Export_Signature_Electronique	Précision sur le format de la signature	Signature XAdES
Objectif	O10.Administration	Précision sur la gestion des politiques de signature	C'est l'application appelante qui peut définir la politique de signature au travers d'un paramètre d'entrée
Objectif	O12.Contrôle_Invariance_Document	Précision	La TOE effectue le contrôle d'invariance
Objectif	O.Lancement_d'Applications_De_Présentation	Suppression	-
Objectif	O13.Présentation_Document	Ajout	La TOE présente elle-même le contenu du document à signer
Objectif	O14.Vérification_Fonctionnement_SCDev	Ajout suite à P14	-
Objectif	OE.Présentation_Document	Suppression	La TOE présente elle-même le contenu du document à signer
Objectif	OE.Contrôle_Sémantique_Document_Signé	Suppression de l'objectif	Le contrôle est effectué par la TOE

Objectif	OE6.Authenticité_Origine_Politique_Signature	Modification au niveau du mot *TOE*	-
Objectif	OE7.Application_Appelante_Sûre	Ajout de l'objectif	-
Objectif	OE8.Administrateur_Développeur_sûr	Ajout de l'objectif	-
Objectif	OE. Administrateur_De_Sécurité_Sûr	Suppression de l'objectif	-
Objectif	OE9.Intégrité_Services	Modification au niveau des mots *administrateur de sécurité*	-
Objectif	OE10.Communication_Web	Ajout de l'objectif sur l'environnement	Le serveur d'application web doit être protégé
Objectif	OE11.Serveur_Web	Ajout de l'objectif sur l'environnement	Les informations doivent transmises de manière sûre
Exigence fonctionnelle de sécurité	FDP_IFF.1/Document acceptance	Assignement	Autres attribut du signataire
Exigence fonctionnelle de sécurité	FDP_IFF.1/Document acceptance	Raffinement	Le contrôle d'invariance est effectué par la TOE
Exigence fonctionnelle de sécurité	FDP_IFF.1/Document acceptance	Suppression de la demande de signer un document instable	En effet, si le document est instable, la TOE ne peut l'afficher et donc le processus de signature est arrêté
Exigence fonctionnelle de sécurité	FDP_ITC.1/Document acceptance	Raffinement	Le contrôle d'invariance est effectué par la TOE
Exigence fonctionnelle de sécurité	FMT_MSA.3/Document's acceptance	Raffinement	La TOE arrête le processus de signature si le document est instable
Exigence fonctionnelle de sécurité	FMT_MSA.1/Selected documents	Raffinement	C'est l'application appelante qui transmet à la TOE le contenu du document à signer
Exigence fonctionnelle de sécurité	FMT_SMF.1/Selection of a list of documents	Raffinement	Un seul document peut être signé par la TOE
Exigence fonctionnelle de sécurité	FMT_SMF.1/Getting document's semantics invariance status	Raffinement	Le contrôle d'invariance est effectué par la TOE
Exigence fonctionnelle de sécurité	FMT_MSA.1/Signer agreement to sign an instable document	Suppression de l'exigence	En effet, la signature sera toujours refusée dans le cas d'un document instable
Exigence fonctionnelle de sécurité	FMT_SMF.1/Getting signer agreement to sign an instable document	Suppression de l'exigence	En effet, la signature sera toujours refusée dans le cas d'un document instable
Exigence fonctionnelle de sécurité	FMT_MSA.1/Signature attributes	Précision sur la gestion des arributs de signature	C'est l'application appelante qui peut définir les attributs de signature au travers d'un paramètre d'entrée

Exigence fonctionnelle de sécurité	FDP_IFF.1/Signer's certificate import	Assignement	Autres attributs du certificat du signataire
Exigence fonctionnelle de sécurité	FDP_MRU.1/Signer's certificate	Assignement	Autres règles concernant les champs du certificat
Exigence fonctionnelle de sécurité	FPT_TDC.1/Signer's certificate	Assignement	Règles d'interprétation d'un certificat
Exigence fonctionnelle de sécurité	FDP_IFF.1/Signature generation	Assignements	a) Autre attribut de signature b) Arrêt de la signature si le document ne peut être présenté
Exigence fonctionnelle de sécurité	FDP_IFF.1/Signature generation	Raffinement	La TOE effectue elle-même l'affichage
Exigence fonctionnelle de sécurité	FDP_IFF.1/Signature generation	Raffinement	a) Il faut aussi que les règles concernant le certificat et décrite par FDP_MRU.1/Signer's certificate soient respectées b) Et que la TOE ait la capacité de transférer les données à signées formatées au SCDev, et de recevoir cette signature de la part du SCDev
Exigence fonctionnelle de sécurité	FDP_MRU.1/Signature attributes Mandatory rules	Modification	La présence de la référence de la politique de signature est obligatoire
Exigence fonctionnelle de sécurité	FDP_ITC.1/Explicit signer agreement	Assignement	Description de ce que le signataire doit effectuer pour donner son consentement explicite à signer un document
Exigence fonctionnelle de sécurité	FDP_IFC.1/Electronic signature export	Raffinement	Précision sur la nature des attributs de signature afin de correspondre à l'objectif de sécurité O5
Exigence fonctionnelle de sécurité	FDP_IFF.1/Electronic signature export	Raffinement	Précision sur la nature des attributs de signature afin de correspondre à l'objectif de sécurité O5
Exigence fonctionnelle de sécurité	FDP_IFF.1/Electornic signature export	Raffinement	Ajout de la capacité de verifier que la signature générée est au format PKCS#1
Exigence	FDP_IFF.1/Electornic signature export	Raffinement	Ajout de la capacité

fonctionnelle de sécurité			de formater la signature au format XAdES
Exigence fonctionnelle de sécurité	FCS_COP.1/Hash function	Assignement	Algorithme de hachage et standard FIPS 180-2
Exigence fonctionnelle de sécurité	FMT_SMR.1 Security roles	Raffinement	L'administrateur de la TOE est changé en l'application appelante
Exigence fonctionnelle de sécurité	FMT_MTD.1/Document format/viewer association table	Raffinement	La table est figée dans la TOE, c'est pourquoi personne ne peut la modifier
Exigence fonctionnelle de sécurité	FMT_SMF.1/Management of the document/format association table	Raffinement	Personne ne peut modifier la table, puisqu'elle est figée dans la TOE
Exigence fonctionnelle de sécurité	FMT_MTD.1/Management of the signature policies	Assignement	Operation possible : "define"
Exigence fonctionnelle de sécurité	FMT_MTD.1/Management of the signature policies	Raffinement	C'est l'application appelante qui peut définir la politique de signature
Exigence fonctionnelle de sécurité	FMT_SMF.1/Management of the signature policies	Assignement	Operation possible : "define"

9. ARGUMENTAIRE

9.1 Argumentaire pour l'ajout des exigences FDP_MRU.1

L'argumentaire pour l'ajout du composant étendu FDP_MRU.1 se décompose en la définition du composant, l'argumentaire proprement dit, et enfin un argumentaire sur sa testabilité.

9.1.1 Définition du composant

La définition générique du composant est la suivante :

Family behaviour

This family addresses security attribute usage and capabilities of access control or information flow control policies when the set of rules to be applied in the policy may vary according to a security attribute.

Component levelling

FDP_MRU Mandatory rules	1

FDP_MRU.1 Mandatory rules is meant to be used to describe the rules required to be implemented by the TOE for supporting the function that implements the SFP as identified in FDP_ACC.

This component should be referred to in the instantiation of an FDP_ACC and/or FDP_IFC component that defines an access control/information flow policy only involving a subset of these rules.

The PP/ST author may iterate this component to address different security attributes or named groups of attributes.

The PP/ST author may also iterate this component to address multiple policies in the TOE.

Management: FDP_MRU.1

There are no management activities foreseen for these components.

Audit: FDP_MRU.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP / ST:

a) Minimal: The invocation of a rule.

FDP_MRU.1 Mandatory rules

Hierarchical to: No other components.

FDP_MRU.1.1 The TSF shall be able to apply a set of rules in enforcing the [assignment: list of access control SFPs or information flow control SFPs].

FDP_MRU.1.2 The TSF shall be able to apply the following set of rules [assignment: list of rules].

Dependencies: [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control]

FMT_MSA.3 Static attribute initialisation

9.1.2 Argumentaire pour l'ajout

L'ajout du composant étendu FDP_MRU.1 a été suscité par le fait que l'ensemble des règles à appliquer dans le cadre des politiques de contrôle de flux définies dans cette cible de sécurité dépendent de la politique de signature, qui n'est a priori pas connue au moment de l'évaluation du produit. Définir les règles à vérifier dans le cadre d'un élément FDP_IFF.1.2 aurait abouti à la définition d'une politique de signature « en dur ».

De plus, ce composant répond aussi à la volonté de définir un ensemble minimal de règles de vérifications implémentées par tous les produits compatibles avec cette cible de sécurité.

9.1.3 Testabilité du composant

Le composant fonctionnel étendu FDP_MRU.1 s'apparente à la fois à FDP_ACF.1 (et FDP_IFF.1) par le fait qu'il définit des règles pouvant être invoquées dans le cadre d'une politique de contrôle d'accès ou d'une politique de contrôle de flux d'information, et à FMT_SMF.1 par le fait qu'il exige qu'un ensemble de fonctions soit fourni par la TSF.

Au final, puisque ses différents aspects sont similaires à des composants bien définis dans la catalogue standard des exigences fonctionnelles de sécurité, il en va de même pour ce composant étendu.

Les éléments d'exigences définis dans le composant étendu FDP_MRU.1 sont donc testables et traçables à travers les différentes représentations de la TOE au même titre que dans les exigences FDP_ACF.1, FDP_IFF.1 et FMT_SMF.1.

9.1.4 Applicabilité des exigences d'assurance

Comme précisé au paragraphe précédent, le composant FDP_MRU.1 s'apparente à la fois aux composants FDP_ACF.1, FDP_IFF.1 et FMT_SMF.1. Pour cette même raison, les exigences d'assurances sont applicables pour supporter la nouvelle exigence fonctionnelle, au même titre que pour les exigences FDP_ACF.1, FDP_IFF.1 et FMT_SMF.1.

10. ANNEXE B – DEFINITIONS

Autorité de certification qualifiée

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

Certificat électronique

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

Un certificat électronique doit comporter :

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

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

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

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

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

f) Le code d'identité du certificat électronique ;

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

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

Certificat électronique qualifié

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

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

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

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

Condensé ou condensat

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

Cryptographic Service Provider (CSP)

En français, fournisseur de services cryptographiques.

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

Dispositif de création de signature électronique

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

Dispositif sécurisé de création de signature électronique

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

Dispositif de vérification de signature électronique

Un matériel ou un logiciel destiné à mettre en application les données de vérification de signature électronique. Directive Directive 1999/93/EC du parlement européen et du conseil du 13 décembre 1999 pour un cadre communautaire sur la signature électronique.

Données de création de signature électronique

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

Données de vérification de signature électronique

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

Format de contenu

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

Object Identifier (OID)

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

Politique de signature

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

Prestataire de services de certification électronique

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

Qualification des prestataires de services de certification électronique

L'acte par lequel un tiers, dit organisme de qualification, atteste qu'un prestataire deservices de certificaion éleconique fournit des prestations conformes à des exigences particulières de qualité.

Signataire

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

Signature électronique

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

Signature électronique sécurisée

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

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

Signature électronique présumée fiable

Une signature mettant en oeuvre 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.