MODULE DE SIGNATURE FASTSIGNATURE

Cible de sécurité (publique)

Version : **1.0**

Référence : **cdc_fastsig_CibleDeSécurité_publique**

Date de la version : **8 décembre 2008**

Société : **CDC FAST**

Confidentialité : **Diffusion publique**

Nombre de pages : **74**

cdc fast

SOMMAIRE

0. ABREVIATION, DEFINITIONS ET DOCUMENTS DE REFERENCE

0.1. Abréviations

AC	Autorité de Certification
CC	Critères Communs
CSP	Cryptographic Service Provider
DCSSI	Direction Centrale de la Sécurité des Systèmes d'Information
DCS	Dispositif de Création de Signature
ETSI	European Telecommunications Standards Institute
OID	Identificateur d'objet (Object IDentifier)
PS	Politique de Signature
PP	Profil de Protection (Protection Profile)
ST	Cible de sécurité (Security Target)
TOE	Cible d'évaluation (Target Of Evaluation)
TSF	Fonctions de sécurité de la cible (Target Security Functions)
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
W3C	World Wide Web Consortium
XAdES	XML Advanced Electronic Signature
XML	eXtended Markup Language
XMLDSIG	XML Digital Signature

0.2. Notations

B.xxx	Bien sensible de la TOE
H.xxx	Hypothèse sur l'environnement de la TOE
M.xxx	Menace pesant sur la TOE
O.xxx	Objectif de sécurité pour la TOE
OE.xxx	Objectif de sécurité pour l'environnement de la TOE
P.xxx	Politique de sécurité organisationnelle

0.3. Définitions

Autorité de Certification	Système de confiance, accepté comme tel par les Partenaires et/ou sous-traitants de CDC FAST, capable de gérer des *certificats électroniques* selon la RFC 3280.
Certificat électronique	Document sous forme électronique attestant du lien en les *données de vérification de signature* et un *signataire*.
Condensat	Résultat d'une fonction hachage
Cryptographic Service Provider (CSP)	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	Matériel ou logiciel destiné à mettre en application les *données de création de signature électronique*.
Dispositif de vérification de signature	Matériel ou logiciel destiné à mettre en application les *données de vérification de signature électronique.*
Données de création de signature	Eléments propres au signataires, tels que des clés cryptographiques privées, utilisés par lui pour créer une *signature électronique.*
Données de vérification de signature	Eléments, tels que des clés cryptographiques publiques, utilisés pour vérifier la *signature électronique*.
OID (Object IDentifier)	Identificateur alphanumérique, enregistré auprès de l'AFNOR pour désigner de manière unique un objet ou une classe d'objets spécifique.
Partenaires et/ou sous-traitant de CDC FAST	Ensemble des parties impliquées dans le service FAST (Collectivité Territoriale, Ministère de l'Intérieur, Préfecture, Autorité de Certification, fournisseur de marques de temps sûres, CDC FAST…)
Politique de Signature	Ensemble des règles pour la création ou la validation d'une signature électronique, sous laquelle une signature peut être déterminée valide.
Signataire	Toute personne physique, agissant pour son propre compte ou pour celui de la personne physique ou morale qu'elle représente, qui met en œuvre un *dispositif de création de signature électronique.*
Signature électronique	Donnée, qui résulte de l'usage d'un procédé répondant aux conditions définies par les lois et règlements en vigueur, destinée à identifier celui qui l'appose et manifester son accord sur le contenu du document au même titre qu'une signature manuscrite.

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.

0.4. Documents de référence

[CC-1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 2.2, January 2004. CCIMB-2004-01-001.
[CC-2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements. Version 2.2, January 2004. CCIMB-2004-01-002.
[CC-3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements. Version 2.2, January 2004. CCIMB-2004-01-003.
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 2.2, January 2004. CCIMB-2004-01-04.
[CRYPT-STD]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse *standard* et *renforcé*, Version 1.0, mai 2004. DCSSI, SGDN/DCSSI/SDS/AsTeC.
[FIPS PUB 180-1]	Federal Information Processing Standards Publication : Secure Hash Standard, FIPS PUB 180-1, http://csrc.nist.gov/publications/fips/fips180-1/fip180-1.pdf
[FIPS PUB 180-2]	Federal Information Processing Standards Publication : Secure Hash Standard, FIPS PUB 180-2, http://csrc.nist.gov/publications/fips/fips180-2/fip180-2.pdf
[QUA-STD]	Processus de qualification d'un produit de sécurité – Niveau standard, Version 1.0, juillet 2003. DCSSI, 001591/SGDN/DCSSI/SDR.
[PKCS #1v1.5]	PKCS #1 v1.5 : RSA Encryption Standard RSA Laboratories, http://www.rsasecurity.com/rsalabs/pkcs/pkcs-1/
[PKCS #1v2.1]	PKCS #1 v 2.5 : RSA Cryptography Standard RSA Laboratories, http://www.rsasecurity.com/rsalabs/pkcs/pkcs-1/
[PP-SIG]	Profil de Protection « Application de création de signature » version 1.0, référence PP-ACSE, 15 février 2005
[PKCS #1v1.5]	PKCS #1 v1.5 : RSA Encryption Standard RSA Laboratories, http://www.rsasecurity.com/rsalabs/pkcs/pkcs-1/
[TS 101 733]	ETSI TS 101 733, Electronic Signature Formats, ETSI Standard, version 1.5.1, décembre 2003.

[TS 101 903]	ETSI TS 101 903,XML Advanced Electronic Signatures (XAdES), v1.2.2 http://uri.etsi.org/01903/v1.2.2#
[TS 101 862]	ETSI TS 101 862, Qualified Certificate Profile, ETSI Standard, version 1.3.1, mars 2004.
[X.509 v3]	IETF RFC 3280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002, http://www.ietf.org/rfc/rfc3280.txt
[XML]	W3C Extensible Markup Language (XML) Recommendation, http://www.w3.org/TR/2000/REC-xml-20001006
[XML-C14EXC]	W3C Exclusive XML Canonicalization Recommendation, http://www.w3.org/TR/2002/REC-xml-exc-c14n-20020718/

1. INTRODUCTION

1.1. Identification de la cible de sécurité et de la cible d'évaluation

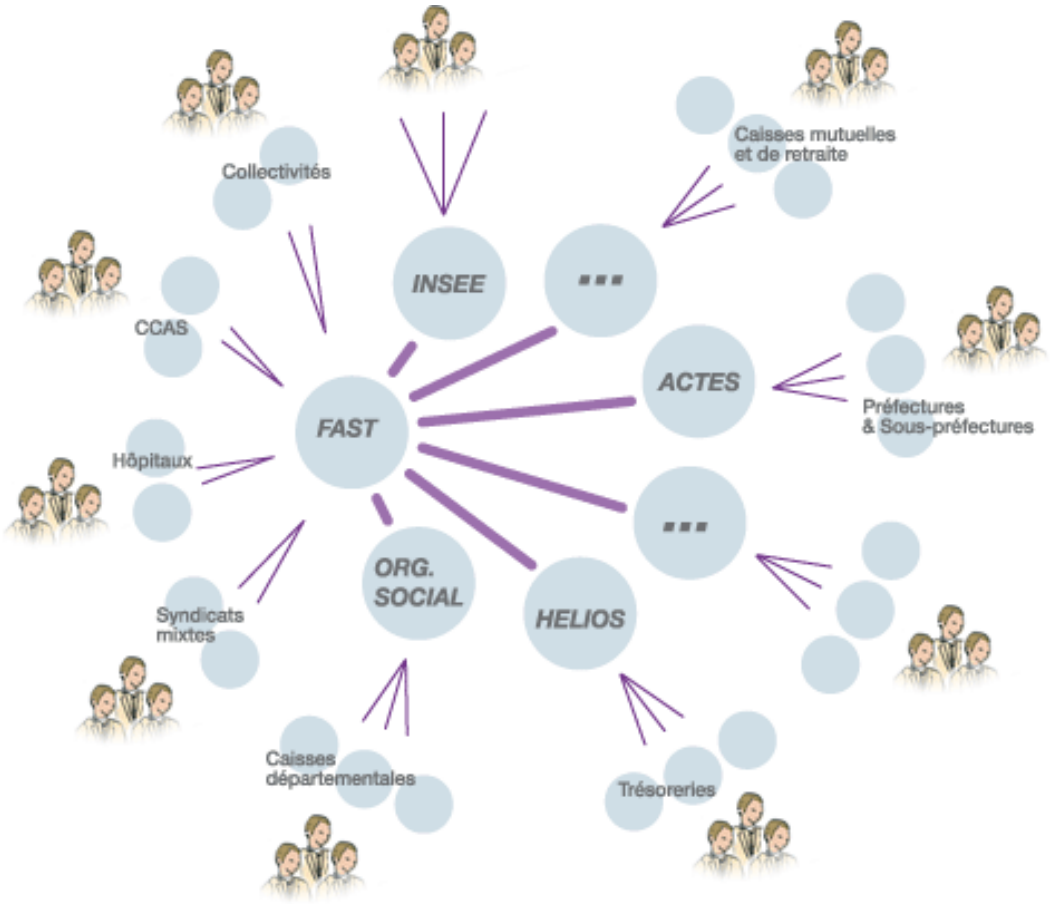
Titre de la ST	Module de signature FASTSignature – Cible de sécurité (publique)
Version de la ST	**1.0**
Identification de la TOE	FASTSignature
Version de la TOE	1.1
Conformité aux CC	La présente cible de sécurité est conforme aux parties 2 (étendue du composant FDP_MRU.1) et 3 des Critères Communs, Version 2.2, avec les interprétations 86, 146, 192, 220, 227, 228, 232, 243.
Conformité à un PP	La cible de sécurité est conforme au PP « Application de création de signature » [PP-SIG].
Niveau d'assurance	Le niveau d'assurance visé est le niveau EAL2 conformément aux parties 2 et 3 des Critères Communs version 2.2, augmenté des composants ADV_HLD.2, ALC_DVS.1, ALC_FLR.3, AVA_MSU.1, AVA_VLA.2 pour l'ensemble de la TOE et des composants ADV_LLD.1, ADV_IMP.1, ALC_TAT.1 pour les fonctions cryptographiques spécifiées au travers de la classe FCS.
Mots clés	Signature électronique, Application de signature électronique, Application de création de signature électronique, XAdES, Signature électronique sécurisée, Signature électronique qualifiée

1.2. Vue d'ensemble de la cible de sécurité

1.2.1. Généralités sur la cible de sécurité

Pour faciliter la modernisation de l'administration et la simplification des démarches citoyennes, la Caisse des Dépôts et Consignations (CDC) s'investit dans la confiance électronique. Cette action l'amène à participer à l'analyse des besoins, l'aménagement des processus organisationnels ou encore la concentration des flux d'échanges administratifs, en liaison avec l'ensemble des partenaires de l'administration électronique. Dans ce cadre, la Caisse des Dépôts et Consignations pilote FAST, et fédère les différents partenaires institutionnels, publics et privés, qui porteront son développement opérationnel. Le site web du projet FAST est consultable à l'adresse : http://www.cdcfast.fr.

FAST (Fournisseur d'Accès Sécurisé Transactionnel) est une infrastructure de confiance spécialisée dans l'envoi des actes administratifs par moyen électronique sécurisé (signature électronique) des collectivités locales vers les administrations centrales, les organes déconcentrés, les organismes sociaux, d'autres collectivités :



Bien au-delà de la solution technologique, FAST accompagne les collectivités locales durant toutes les étapes de la démarche avec une assistance-conseil personnalisée, la formation du personnel, une hot-line utilisateurs.

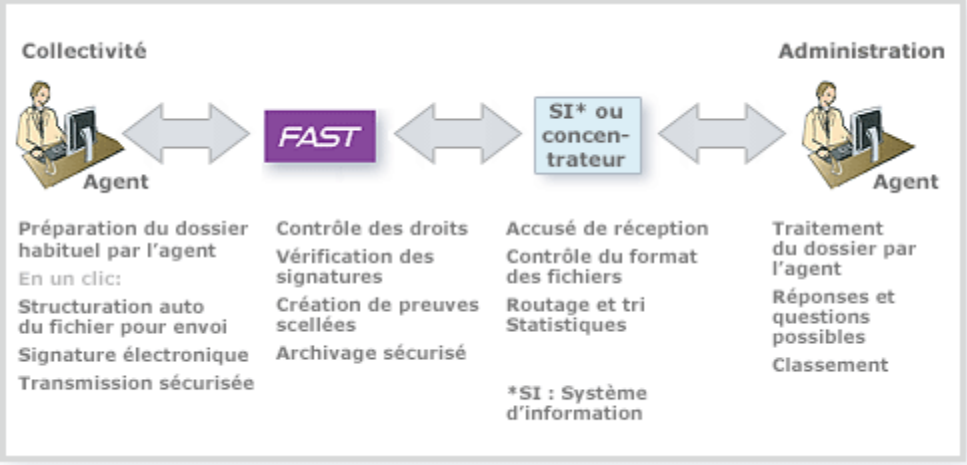
FAST développe et intègre trois facteurs clés assurant le succès de l'ADministration ÉLEctronique :

1. **Fédérer :**
   - Utiliser les normes et standards permettant de communiquer électroniquement entre l'État et les collectivités,
   - Concentrer les échanges entre des systèmes logiciels différents, sur une même plate-forme technique totalement interopérable,
   - Enrichir les logiciels métier des collectivités d'interfaces évitant toute ressaisie.
2. **Déployer :**
   - Faciliter la mise en place et la connexion des collectivités à l'infrastructure de confiance,
   - Former les utilisateurs à son utilisation simple, en tenant compte des outils existants,

- Assistance et support aux utilisateurs, indispensables à un déploiement général sur tout le territoire.

3. **Garantir :**
    - Assurer une pérennité dans les services et leur maintenant sur le très long terme,
    - Sécuriser l'acheminement des informations (particulièrement sur les données personnelles),
    - Tracer et prouver la totalité des échanges,
    - N'exclure aucun métier administratif de l'utilisation de l'infrastructure de confiance.

Dans le cadre du projet FAST, la CDC a développé un ensemble d'interfaces de programmation mises à disposition des éditeurs et des organismes souhaitant se raccorder à la plate-forme, afin de faciliter l'intégration des fonctionnalités de télétransmission au sein de leurs progiciels métier ou de leurs systèmes d'information :



Les fonctionnalités offertes sont regroupées en quatre grandes familles fonctionnelles :

- FAST Signature : création de signatures électroniques
- FAST Chiffrement : chiffrement / déchiffrement de données
- FAST Formatage : formatage d'enveloppes d'échange FAST
- FAST Echange : échanges sécurisés avec la plate-forme FAST

Le tableau ci-dessous présente les différents *packagings* et environnement sous lesquels ces interfaces de programmations sont mises à disposition des développeurs métier :

	Packaging	**Windows** (W98, WNT, W2K, WXP)	**Unix** (Solaris, Linux, AIX, HP/UX)
Signature	API C	Oui	Oui
	Objet COM	Oui	-
	Classe JAVA	Oui	Oui
Chiffrement	API C	Oui	Oui
	Objet COM	Oui	-
	Classe JAVA	Oui	Oui
Formatage	API C	Oui	Oui
	Objet COM	Oui	-
	Classe JAVA	Oui	Oui
Echange	API C	Oui	Oui
	Objet COM	-	-
	Classe JAVA	Oui	Oui

La cible d'évaluation FASTSignature est un module logiciel permettant de créer des signatures électroniques au format européen XAdES en s'appuyant sur un dispositif de création de signature effectuant les calculs cryptographiques mettant en œuvre la clé privée du signataire. Ce module logiciel se présente sous la forme d'un contrôle ActiveX.

Bien que la certification de l'outil ne soit pas requise pour bénéficier de la présomption de fiabilité au sens du décret n°2001-272 du 30 mars 2001, CDC FAST souhaite recourir à cette certification afin d'améliorer la sécurité de la chaîne de signature mise en œuvre dans le cadre du projet FAST et de disposer de preuves complémentaires en cas de contestation de la signature démontrant que le procédé de signature utilisé n'est pas fiable (c'est-à-dire d'apport par un tiers contestataire d'un preuve contraire remettant en cause la présomption de fiabilité de la signature).

FASTSignature permet la génération de la signature d'un document et d'attributs afférents à la signature avec une clé privée associée à un certificat propre au signataire et confinée dans un dispositif de création de signature (dénommé SCDev).

FASTSignature permet de créer au mieux des signatures électroniques présumées fiables (ou signatures électroniques qualifiées au sens de la Directive) lorsque qu'il est utilisé avec des certificats qualifiés et un dispositif sécurisé de création de signature (SSCD), et au moins des signatures électronique sécurisées (ou signatures électroniques avancées au sens de la Directive).

Les calculs cryptographiques mettant en œuvre la clé privée du signataire et permettant ainsi de créer la signature sont réalisés dans le dispositif de création de signature (dénommé SCDev).

1.2.2. Répartition des rôles

La répartition des rôles dans le processus d'évaluation est le suivant :

Organisme de certification	DCSSI
Commanditaire	CDC Numérique
Développeur	DICTAO
CESTI Evaluateur	OPPIDA

1.2.3. Conformité aux Critères Communs

Conformité aux CC	La présente cible de sécurité est conforme aux parties 2 (étendue du composant FDP_MRU.1) et 3 des Critères Communs, Version 2.2 avec les interprétations suivantes : • RI # 86 – Role of Sponsor ; • 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 PP « Application de création de signature » [PP-SIG]. Les ajouts par rapport au profil de protection sont indiqués en rouge, et les suppressions en ~~rouge barré~~.
Niveau d'assurance	Le niveau d'assurance visé est EAL2 Augmenté. L'augmentation des composants d'assurance porte : • Pour l'ensemble de la TOE sur les tests de vulnérabilité (AVA_VLA.2), la conception de haut niveau du produit (ADV_HLD.2), la qualité de sa documentation (AVA_MSU.1), sa maintenance (ALC_FLR.3) et la sécurité des développements (ALC_DVS.1). • Pour les fonctions cryptographiques spécifiées au travers de la classe fonctionnelle FCS sur leur conception de bas niveau (ADV_LLD.1), la représentation de leur implémentation (ADV_IMP.1) et les outils de développement utilisés (ALC_TAT.1). Ce paquet d'assurance répond aux exigences définies pour la 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 » (Strength of Functions High).

1.2.4. Organisation du document

La présente cible de sécurité est constituée des chapitres suivants :

- Description de la cible d'évaluation (Chapitre 2) : fournit une description de la cible d'évaluation dans le but d'en clarifier le fonctionnement.
- Environnement de sécurité de la cible d'évaluation (Chapitre 3) : décrit les menaces, les politiques de sécurité organisationnelles et les hypothèses s'appliquant à la TOE.
- Objectifs de sécurité (Chapitre 4) : identifie les objectifs de sécurité satisfaits par la TOE et par son environnement.
- Exigences de sécurité (Chapitre 5) : présente les exigences fonctionnelles de sécurité et les exigences d'assurance portant sur la TOE
- Spécifications globales de la cible d'évaluation (Chapitre 6) : décrit les fonctions de sécurité implémentée par la TOE et les mesures d'assurance de la TOE pour satisfaire les exigences fonctionnelles et d'assurance et les objectifs de sécurité.
- Conformité à un profil de protection (Chapitre 7) : présente l'argumentaire pour la conformité de la cible de sécurité avec le profil de protection [PP-SIG].
- Argumentaire (Chapitre 8) : présente l'argumentaire pour les objectifs et les exigences de sécurité.

2. DESCRIPTION DE LA CIBLE D'EVALUATION

Cette section fournit une description de la cible d'évaluation dans le but d'en clarifier le fonctionnement.

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

Les plates-formes utilisées pour l'évaluation sont présentées au paragraphe 2.3.1. Par la suite, nous entendrons par plate-forme le triplet machine, système d'exploitation et navigateur Internet.

2.1. Description générale

La cible d'évaluation est le module logiciel FASTSignature permettant de créer des signatures électroniques au format européen XAdES [TS 101 903] sur un document au format XML, en s'appuyant sur un dispositif de création de signature (hors périmètre d'évaluation) effectuant les calculs cryptographiques mettant en œuvre la clé privée du signataire. La signature électronique XAdES créée est elle-même structurée au format XML et est directement insérée dans le document XML à signer. On parle de signature enveloppée (*enveloped signature*).

Le module FASTSignature se présente sous la forme d'un contrôle ActiveX.

Le dispositif de création de signature peut se présenter sous plusieurs formes, parmi lesquelles une carte à puce, un token USB ou encore sous forme logicielle au travers d'un fichier au format PKCS #12. Il sera aussi nommé SCDev dans la suite du document, pour Signature Creation Device.

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 de cette manière.

Les documents signés par la TOE sont au format XML sous forme canonique (suivant l'algorithme C14N exclusif). Ce format est invariant (cf §2.2.4) par nature. La TOE réalise l'affichage de ces documents grâce à une transformation du contenu XML du document en HTML. La correspondance entre les balises XML et leur équivalent en HTML est effectuée à l'aide d'une table de correspondance présente dans un fichier[1]. Dans le cas où la TOE ne peut pas afficher le document (cf §2.2.3), elle arrête le processus de signature.

2.2. Périmètre et architecture

2.2.1. Représentation physique

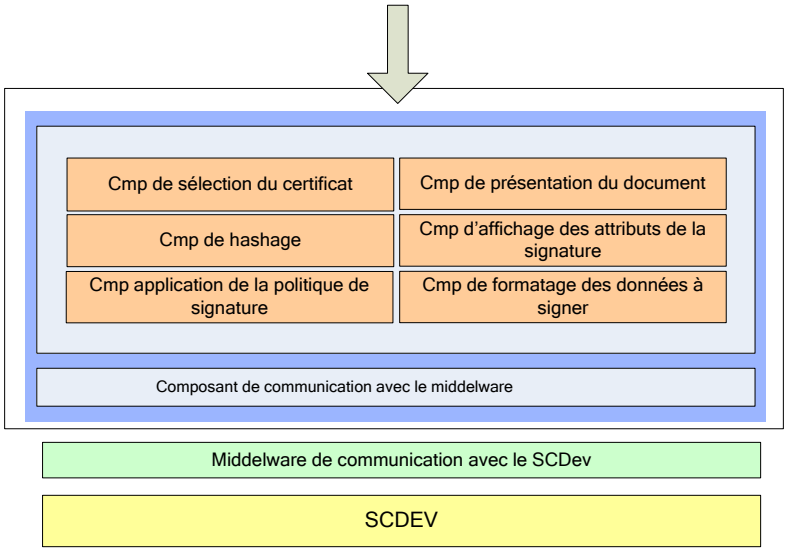
La TOE se présente sous la forme d'un fichier ayant l'extension .cab.

Les plates-formes (hors périmètres) sur lesquelles est évalué le produit sont définies au paragraphe §2.3.1.

[1] Une documentation est fournie indiquant la syntaxe de ce fichier de correspondance.

2.2.2. 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 : l'appel du module par l'application appelante, le middleware de communication avec le SCDev et le SCDev lui-même.



La TOE présente un certain nombre d'interfaces. Il s'agit :

- Soit d'interfaces homme-machine permettant au signataire d'interagir directement avant la TOE (sélection du certificat de signature, visualisation des attributs de signature…)
- Soit d'interfaces programmatiques (API) permettant à une application appelante de jouer le rôle d'interface entre le signataire et la TOE (sélection du document à signer, sélection de la politique de signature à appliquer…)

Le document à signer est transmis à la TOE par l'application appelante au travers d'une interface programmatique.

Le document à signer doit être sous forme canonique et encodé en UTF-8, conformément aux recommandations du W3C [XML-C14EXC]. Si le document n'est pas déjà sous forme canonique, c'est à l'application appelante de procéder à l'opération préalablement à la transmission du document à la TOE pour signature.

Remarque relative à la mise sous forme canonique : la spécification du format XML 1.0 permet d'écrire les mêmes informations utiles de plusieurs manières. Ces variations portent sur des détails syntaxiques tels que l'encodage utilisé, l'ordre relatif des attributs dans les balises, le caractère (simple ou double apostrophe) utilisé pour délimiter les valeurs d'attributs, etc. Les usages et décisions d'implémentation des parseurs XML ont fait en sorte que dans certains cas les outils XML n'ont pas les moyens de déterminer quelles options ont été choisies pour exprimer les informations pouvant s'exprimer de plusieurs manières.

Ainsi un outil XML lisant un document pour apporter une modification même mineure est généralement incapable de préserver l'ensemble des options initiales lors de sa réécriture : une apostrophe simple dans le fichier lu peut ainsi être remplacée par une apostrophe double dans le fichier de sortie. Afin de pallier ce problème bloquant pour la manipulation de document XML signés, la recommandation XML Signature du W3C définit des algorithmes de mise sous forme canonique permettant de normaliser le document XML préalablement à la signature. L'algorithme devant être appliqué au document à signer par FASTSignature est l'algorithme C14N exclusif, dans sa variante sans conservation des commentaires.

2.2.2.1. Composant de présentation de documents

La TOE peut présenter le document à signer à l'utilisateur :

- Soit sous sa forme XML brut ;
- Soit sous la forme d'un document HTML.

Cette dernière est effectuée car le contenu XML du document n'est pas nécessairement « intelligible » pour un utilisateur. Ainsi, le TOE effectue, grâce à une table de correspondance entre les balises XML et leur équivalent HTML, la transformation du contenu, afin de le rendre plus accessible.

Cette table de correspondance se trouve dans un fichier. La table est statique.

L'affichage du document sous sa forme XML ou sa forme HTML est entièrement effectué par la TOE.

Dans le cas où la table de correspondance définit une balise HTML que la TOE ne saurait affichée, ou dans le cas où une balise XML du document à signer n'aurait pas d'équivalent HTML, la TOE avertit l'application appelante et arrête le processus de signature.

2.2.2.2. Composant d'application de la politique de signature

La TOE utilise des politiques de signature sous forme de fichiers interprétables par la TOE. La sélection de la politique de signature adéquate se fait sur la base du nom de l'application métier concernée et du rôle du signataire. Une politique de signature permet ainsi de préciser, pour une application métier et pour un rôle donnés (transmis par l'application appelante) les informations définies au paragraphe § 2.2.5.

À toute politique de signature sélectionnée viennent s'ajouter un certain nombre d'exigences complémentaires stockées sous forme de code exécutable dans la TOE (politiques fixes) :

- Le certificat autorise l'usage de la clé privée pour des opérations de signature
- Le certificat est dans sa période de validité.

2.2.2.3. Composant de sélection du certificat

Le certificat de signature sélectionné doit répondre aux critères suivants :

- Le certificat est conforme à la norme X.509v3 [X.509 v3] ;
- L'autorité de certification émettrice du certificat est une autorité référencée ;
- Le certificat autorise l'usage de la clé privée pour des opérations de signature ;
- Le certificat est dans la période de validité.

La TOE propose plusieurs modes de sélection du certificat de signature :

- De façon transparente pour le signataire dans le cas où l'application appelante fournit le certificat à la TOE au travers d'une interface programmatique. Un contrôle est ensuite effectué par la TOE sur ce certificat pour s'assurer qu'il répond bien aux critères énoncés en début de paragraphe. Dans ce mode, le Common Name (CN) du sujet du certificat et celui de l'autorité de certification sont tout de même affichés à l'utilisateur, ce dernier pouvant accéder à une représentation complète du certificat au travers d'une fenêtre.
- En permettant au signataire de sélectionner lui-même, au travers d'une interface homme-machine, un certificat de signature. Cette sélection se fait parmi la liste des certificats proposés par le SCDev répondant aux critères énoncés au chapitre précédent.
  La fenêtre de sélection présente, pour chacun des certificats :
  - Le Common Name (CN) du sujet du certificat
  - Le Common Name de l'autorité de certification émettrice du certificat

L'utilisateur peut accéder à une représentation complète du certificat au travers d'une seconde fenêtre.

2.2.2.4. Composant d'affichage des attributs de la signature

La TOE permet au signataire de visualiser les attributs de signature sélectionnés avant d'engendrer la signature. Les informations présentées au signataire sont définies au paragraphe §2.2.6.

2.2.2.5. Composant de formatage des données à signer

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

Il effectue les opérations suivantes :

- Insertion du modèle de signature au format XAdES dans le document XML à signer (rappel : l'outil produit des signatures « enveloppées »).
- Formatage et intégration des attributs de la signature sélectionnés dans les propriétés signées de la signature
- Calcul de la référence sur le document à signer
- Calcul de la référence sur les propriétés signées de la signature

2.2.2.6. Composant de hachage

Les algorithmes implémentés par la TOE sont des algorithmes de hachage conformes au niveau standard définit dans [CRYPT-STD] :

- SHA-1 [FIPS PUB 180-1]
- SHA-256 [FIPS PUB 180-2]

L'algorithme de hachage est sélectionné par l'application appelante. Ce même algorithme est utilisé pour toutes les opérations de calcul de condensat effectuées par la TOE pour créer la signature, en particulier :

- Lors des calculs intermédiaires des références de la signature XAdES
- Lors du calcul du condensat des données à signer

2.2.2.7. Composant de communication avec le dispositif de création de signature

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

Le composant de pilotage de l'interface avec le SCDev assure les fonctions suivantes, par l'intermédiaire du fournisseur de services cryptographiques matérialisant l'interface avec le SCDev :

- Obtenir du SCDev la liste des certificats utilisables par le signataire
- Indiquer au SCDev la clé de signature à activer
- Transférer le condensat formaté des données à signer au SCDev
- 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

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

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

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

- en permettant au signataire de visualiser le document à signer ;
- en ne signant que des documents au format XML sous forme canonique selon l'algorithme C14N exclusif sans conservation des commentaires, dont la sémantique ne peut varier ;
- enfin, en permettant au signataire de visualiser les attributs qui seront signés conjointement avec le document.

FASTSignature effectue l'affichage du document et des attributs de signature.

L'affichage du document est effectué grâce à une table de correspondance entre les balises XML et un équivalent en HTML. La TOE affiche ensuite le contenu HTML. Seules certaines balises HTML sont reconnues comme permettant de s'assurer de la stabilité du document sous sa forme HTML.

Dans le cas où la TOE ne peut afficher le document, le processus de signature est arrêté.

2.2.4. Contrôle de l'invariance sémantique et présentation du document

Le document à signer pourrait 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.

Cependant, la TOE signe des documents au format XML, préalablement mis sous forme canonique, par l'application appelante, suivant l'algorithme C14N exclusif, dans sa variante sans conservation des commentaires. La sémantique de ce type de document est stable par nature, c'est pourquoi aucun contrôle d'invariance sémantique sur le document n'est nécessaire.

Par construction FASTSignature ne pourra donc signer un document XML dont la sémantique est jugée instable. C'est pourquoi d'une part, aucun contrôle de stabilité n'est effectué et, d'autre part, la politique de signature ne comporte pas de paramètre « permettre ou non de signer un document instable ».

2.2.5. La politique de signature

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

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

La politique de signature comprend les informations suivantes :

- Les informations caractérisant la politique de signature déterminée en fonction du rôle présumé du signataire :
    - Une description littérale de la politique de signature
    - Une URL permettant de récupérer une version complète (et signée) de la politique de signature
    - Une référence non ambiguë à la politique de signature, constituée :
        - d'un condensat la politique de signature, et de
        - l'identifiant de l'algorithme de hachage utilisé pour calculer le condensat.
- Les certificats des autorités de certification référencées
- L'algorithme de hachage à utiliser pour générer la signature (cf §2.2.2.6)
- 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
- le type d'engagement (conforme aux types d'engagement définis dans le document [TS 101 733])

2.2.6. Les attributs de signature

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

- Les informations caractérisant la politique de signature déterminée en fonction du rôle présumé du signataire :
    - Une description littérale de la politique de signature
    - Une URL permettant de récupérer une version complète (et signée) de la politique de signature
    - Une référence non ambiguë à la politique de signature, constituée :
        - d'un condensat la politique de signature, et de
        - l'identifiant de l'algorithme de hachage utilisé pour calculer le condensat.
- le rôle du signataire
- les informations caractérisant le certificat de signature sélectionné par le signataire :
    - Le nom de l'autorité de certification émettrice du certificat de signature
    - Le numéro de série du certificat de signature
- Une référence non ambiguë au certificat de signature, constituée :
    - d'un condensat du certificat, et de
    - l'identifiant de l'algorithme de hachage utilisé pour calculer le condensat.
- la date et l'heure présumées de la signature déterminée par la TOE à partir de l'heure système de la machine hôte
- le lieu de signature
- le type d'engagement (conforme aux types d'engagement définis dans le document [TS 101 733])

2.2.7. Le format XAdES

Le standard DSig (Digital Signature) spécifie la syntaxe XML et les règles de traitement pour créer et représenter des signatures digitales. 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 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).

2.3. Plate-forme d'évaluation

L'environnement de la cible d'évaluation est composé des éléments suivants :

- la plate-forme hôte ;
- les composants logiciels permettant de communiquer avec le dispositif de création de signature (SCDev) ;
- un dispositif de création de signature électronique ;
- un document XML représentatif et la table de correspondance associée

2.3.1. La plate-forme 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 un ordinateur personnel (de type PC) selon les configurations suivantes :

Systèmes d'exploitation :

- Windows XP
- Windows Server 2003

Navigateur Internet :

- Internet Explorer version 6.0

Dispositifs de création de signature :

- SCDev logiciel du Navigateur
- Carte à puce + Lecteur ActiveCard

	Carte à puce ActivCard	SCDev logiciel
Windows XP / IE 6.0	✓	✓
Windows Server2003 / IE 6.0	✓	✓

Tableau 1 - Tableau résumant les configurations évaluées

2.3.2. Le fournisseur de services cryptographiques

Le fournisseur de services cryptographiques fournit les interfaces permettant l'interfaçage entre la TOE et le SCDev. Il s'agit d'un composant logiciel intégré au système d'exploitation de la machine hôte permettant à une application d'interagir avec un SCDev.

2.3.3. Le dispositif de création de signature

Les dispositifs de création de signature (ou SCDev) supportés par la TOE sont ceux disposant d'un fournisseur de services cryptographiques (CSP) supporté par la plate-forme hôte.

Le SCDev peut être logiciel (dispositif intégré au système d'exploitation de la machine hôte) ou matériel (carte à puce ou token).

Deux SCDev différents sont utilisés au cours de l'évaluation, à savoir :

- Le SCDev logiciel intégré directement dans le système d'exploitation. Dans ce cas le fournisseur de services cryptographiques utilisé est celui nativement embarqué dans le système d'exploitation. Il s'agit du *Enhanced Cryptographic Service Provider* de Microsoft.
- Le SCDev matériel [Carte ou token qualifié ou en cours de qualification]. Dans ce cas le fournisseur de services cryptographiques adéquat, est installé par l'administrateur lors de l'installation du SCDev sur la machine hôte.

3. ENVIRONNEMENT DE SECURITE DE LA CIBLE D'EVALUATION

3.1. Biens

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

3.1.1. Biens à protéger par la TOE

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

3.1.1.1. Documents à signer

B.Document_A_Signer ~~Ensemble_Des_Documents_A_Signer~~	D	**I**	C
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.~~ *Note d'application* On entend ici par document : • soit simplement un document électronique • soit un document électronique avec une ou plusieurs signatures imbriquées attachées au document.			
Note FAST Dans le cadre de cette cible, l'ensemble des documents à signer est composé d'un unique document électronique au format XML.			

3.1.1.2. Représentation des données à signer

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

Elles requièrent une protection en intégrité.

B.Données_A_Signer	D	**I**	C
Les données à signer sont les informations sur lesquelles portera la signature ; Elles comprennent : • Le document à signer • Les attributs de la signature sélectionnés par le signataire explicitement ou			

	implicitement par l'application. Les attributs de la signature ~~*doivent* comporter~~ comportent les données suivantes : • ~~Le certificat du signature ou~~ une référence non ambiguë de ce certificat. ~~Ils *peuvent* comporter :~~ • ~~La référence à la politique de signature~~ • ~~Le type d'engagement~~ • ~~Le lieu présumé de la signature~~ • ~~La date et l'heure présumées de la signature~~ • ~~Le format du contenu~~ • ~~….~~
Note FAST	Les attributs de la signature créée par l'outil FASTSignature comportent : • Les informations caractérisant la politique de signature déterminée en fonction du rôle présumé du signataire : o Une description littérale de la politique de signature o Une URL permettant de récupérer une version complète (et signée) de la politique de signature o Une référence non ambiguë à la politique de signature, constituée : ▪ d'un condensat la politique de signature, et de ▪ l'identifiant de l'algorithme de hachage utilisé pour calculer le condensat. • le rôle du signataire • les informations caractérisant le certificat de signature sélectionné par le signataire : o Le nom de l'autorité de certification émettrice du certificat de signature o Le numéro de série du certificat de signature • Une référence non ambiguë au certificat de signature, constituée : o d'un condensat du certificat, et de o l'identifiant de l'algorithme de hachage utilisé pour calculer le condensat. • la date et l'heure présumées de la signature déterminée par la TOE à partir de l'heure système de la machine hôte • le lieu de signature • le type d'engagement (conforme aux types d'engagement définis dans le document [TS 101 733])

B.Données_A_Signer_Formatées	D	**I**	C
Ces données correspondent à un premier formatage des données à signer (enveloppe).			

B.Condensé_Des_Données_A_Signer	D	I	C
	Cette donnée est un condensé des *données à signer formatées*.		

B.Condensé_Formaté	D	I	C
	Ce bien correspond au *condensé des données à signer* après avoir subi un formatage, préalablement à son envoi vers le SCDev.		
Note FAST	Dans le cadre de cette cible le *condensé formaté* est identique au *condensé des données à signer*. Aucun formatage ou padding n'étant appliqué au *condensé des données à signer* préalablement à son envoi vers le SCDev.		

3.1.1.3. Données retournées par la TOE

B.Signature_Electronique	D	I	C

	La signature électronique est une enveloppe comprenant :
	• ~~Le condensé de l'ensemble des données à signer~~
	• La signature numérique au format XAdES, comprenant :
	  • La signature numérique du document;
	  • Le condensé de l'ensemble des données à signer;
	  • Le certificat du signataire lui-même;
	  • Une référence à la politique de signature appliquée
	• ~~Des informations supplémentaires pouvant faciliter la vérification de signature~~
	Ce bien doit être protégé par la TOE au cours de sa constitution avant qu'il soit transmis au signataire.		

3.1.2. Biens sensibles de la TOE

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

B.Politique_De_Signature	D	I	C

	La TOE réalise la signature selon une politique de signature, comprenant les éléments suivants :
	• Les informations caractérisant la politique de signature déterminée en fonction du rôle présumé du signataire :
	  o Une description littérale de la politique de signature
	  o Une URL permettant de récupérer une version complète (et signée) de la politique de signature		

	o Une référence non ambiguë à la politique de signature, constituée : ▪ d'un condensat la politique de signature, et de ▪ l'identifiant de l'algorithme de hachage utilisé pour calculer le condensat. • Les certificats des autorités de certification référencées • L'algorithme de hachage à utiliser pour générer la signature • Le rôle du signataire (inclus dans les données à signer) • Le lieu de signature (inclus dans les données à signer) • Le type d'engagement • Le certificat est utilisable ou non pour des applications de non répudiation

B.Services	D	**I**	C
	Ce bien représente le code exécutable implémentant les services rendus.		

B.Correspondance_Entre_Représentation_De_Données	D	**I**	C
	Les données internes à la TOE possèdent souvent une représentation différente de celles présentées au signataire ou entrées dans la TOE. Ex 1: le type d'engagement (ex: "lu et approuvé") du signataire peut par exemple être représenté en interne par un OID alors qu'il est présenté explicitement au signataire dans l'interface. Ex 2: le format du document entré dans la TOE peut lui aussi être représenté en interne sous la forme d'un OID.		

~~**B.Correspondance_FormatDoc_Application**~~	~~D~~	~~**I**~~	~~C~~
	~~Ce bien est un paramètre géré par la TOE qui lui permet de décider quelle application de présentation externe lancer en fonction du format du document devant être présenté au signataire.~~		
Note FAST	Inutile dans le cas de la présente TOE.		

3.2. Sujet

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

S.Administrateur_De_Sécurité	
	L'administrateur de sécurité de la TOE et d'application appelante est en charge des opérations suivantes : • ~~Gestion de la correspondance entre les formats de document autorisés et les applications permettant leur présentation au signataire~~ • ~~Gestion du paramètre de configuration déterminant si la TOE peut signer un document jugé instable.~~ • Dans le cas où la TOE utilise des politiques de signature paramétrables, gestion la liste des politiques de signature utilisables par la TOE. *Note d'application* Le rôle d'administrateur de sécurité de la TOE est bien distingué du rôle d'administrateur de la machine sur laquelle elle s'exécute (voir l'hypothèse H.Machine_Hôte)

S.Développeur_Application_Appelante	
	Sujet en charge du développement de l'application utilisatrice de la TOE.

S.Application_Appelante	
	L'application appelant la TOE. Elle transmet à la TOE la politique de signature à appliquer.

3.3. Hypothèses

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

3.3.1. Hypothèses sur l'environnement d'utilisation

3.3.1.1. Hypothèses sur la machine hôte

H.Machine_Hote	
	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 : • La machine hôte est protégée contre les virus • Les échanges entre la machine hôte et d'autres machines via un réseau ouvert sont contrôlés par un pare feu contrôlant et limitant les échanges • L'accès aux fonctions d'administration de la machine hôte est restreint aux seuls administrateurs de celle-ci (différenciation compte utilisateur/administrateur) • L'installation et la mise à jour de logiciels sur la machine hôte est sous le contrôle de l'administrateur. Les moyens nécessaires au contrôle de l'intégrité de la TOE sont mis à sa disposition • Le système d'exploitation de la machine hôte refuse l'exécution d'applications téléchargées ne provenant pas de sources sûres *Note d'application* Le rôle d'administrateur de la machine hôte mentionné ci-dessus est à différencier par rapport au rôle d'administrateur de sécurité de la TOE qui a des prérogatives particulières vis-à-vis de la gestion des biens sensibles de la TOE et de ses paramètres de configuration.

3.3.1.2. Hypothèses relatives au dispositif de création de signature

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

H.Dispositif_De_Creation_De_Signature	
	On suppose que le SCDev a notamment pour fonction de générer effectivement la signature à partir des éléments communiqués par la TOE. On suppose de plus qu'il est en charge de l'authentification du signataire pour lui permettre ou non d'utiliser la clé privée correspondant au certificat sélectionné. Le SCDev est ainsi directement en charge de la protection des données propres au signataire. Les données suivantes sont supposées être stockées et utilisées de manière sûre par le SCDev : • Biens relatifs à la génération de la signature o La(les) clé(s) privée(s) du signataire, protégées en confidentialité et en intégrité o Le(s) certificat(s) du signataire, protégés en intégrité, à défaut une référence non ambiguë à ce(s) certificat(s),

	o L'association clé privée/certificat, protégée en intégrité • Biens relatifs à l'authentification du signataire o Les données d'authentification du signataire, protégées en intégrité et en confidentialité. o L'association entre des données d'authentification et le couple clé privée/certificat, protégée en intégrité (1) (1) A noter que l'association peut porter sur une donnée d'authentification et un couple clé privée/certificat. Ainsi, plusieurs couples peuvent être stockés dans le même SCDev. On peut imaginer que leur accès soit protégé par des données d'authentification différentes.

H.Communication_TOE/SCDev	
	On suppose que l'ensemble des composants logiciels et/ou matériels assurant l'interface entre la TOE et le SCDev est capable de gérer (ouvrir / fermer) un canal de communication garantissant l'intégrité et l'exclusivité de la communication. *Note d'application* L'ensemble des composants assurant la communication entre la TOE et le SCDev peut être composé de différents composants logiciels et/ou matériels installés sur le système d'exploitation (ex: les pilotes PKCS #11 ou des fournisseurs de services cryptographiques (CSP) définissant une interface cryptographique que la TOE appelle pour accéder à un dispositif générant effectivement la signature).
Note FAST	Dans le cadre de cette cible de sécurité un composant logiciel appelé fournisseur de services cryptographique (CSP) matérialise cette interface de communication entre la TOE et le SCDev.

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

3.3.1.3. 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 :~~ • ~~Soit retranscrivent fidèlement le type du document à signer,~~ • ~~Soit préviennent le signataire des éventuels problèmes d'incompatibilités du dispositif de présentation avec les caractéristiques du document.~~

Note FAST	La TOE effectue elle-même l'affichage du document

~~**H.Présentation_Signatures_Existantes**~~	
	~~Dans le cas d'une contre-signature, on suppose que le signataire dispose d'un moyen de connaître au moins l'identité du ou des signataires précédents, et au mieux vérifie cette ou ces signatures.~~
Note FAST	La TOE ne signe pas de document déjà signé.

3.3.1.4. Hypothèses concernant l'invariance 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 FAST	Le type de document signé par la TOE est au format XML sous forme canonique suivant l'algorithme C14N exclusif sans conservation de commentaire. Ce format est invariant par nature. Aucun contrôle d'invariance de sémantique n'est nécessaire.

3.3.2. Hypothèses sur le contexte d'utilisation

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

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

H.Développeur_Application_Appelante_Sûr	
	Le développeur de l'application appelante est supposé être de confiance, formé à l'utilisation de la TOE et disposant des moyens nécessaires à la réalisation de son activité.

H.Application_Appelante_Sûre	
	L'application appelante est supposée être développée conformément au guide de développement (cf. § 6.2.4.2 Guide pour le développement d'applications externes). Elle s'assure en particulier de la mise sous forme canonique du document à signer, selon l'algorithme C14N exclusif sans conservation de commentaire.

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

H.Politique_De_Signature_d'Origine_Authentique	
	L'origine de la ou les politiques de signature utilisables par la TOE est supposée authentique.

H.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.

H.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: • le serveur est protégé contre les virus • les échanges entre la machine hôte et d'autres machines via un réseau ouvert sont contrôlés par un pare feu contrôlant et limitant les échanges • l'accès aux fonctions d'administration 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

3.4. Menaces

Il n'y a pas de menace sur la TOE.

3.5. Politiques de sécurité organisationnelles

Cette section définit les règles d'ordre organisationnel applicables à la TOE.

3.5.1. Politiques relatives à la validité de la signature créée

P.Conformité_Certificat_Signataire	
	Pour éviter la création de signatures invalides, la TOE doit contrôler que le certificat sélectionné par le signataire est bien conforme à la Politique de Signature à appliquer.

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

P.Conformité_Attributs_Signature	
	Pour éviter la création de signatures invalides, la TOE doit contrôler : • Que les attributs de signature sélectionnés par le signataire sont bien conformes à la politique de signature à appliquer, et • Que tous les attributs de signature requis par la politique de signature sont présents.

3.5.2. Contrôle de l'invariance de la sémantique du document

~~**P.Sémantique_Document_Invariante**~~	
	~~La TOE doit informer le signataire si la sémantique du document n'a pu être déterminée comme étant stable.~~ ~~Selon la politique de signature, la TOE adopte l'un ou l'autre des comportements suivants, si la sémantique du document n'était pas déterminée comme stable :~~ • ~~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 FAST	Le type de document que signe la TOE est au format XML sous forme canonique suivant l'algorithme C14N exclusif sans conservation de commentaire. Ce type est invariant par nature. Aucun contrôle d'invariance de sémantique n'est nécessaire.

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

P.Possibilité_De_Présenter_Le_Document	
	La TOE doit permettre au signataire d'accéder à une représentation fidèle du document à signer. La TOE ne permettra pas la signature d'un document s'il ne peut pas être présenté au signataire.

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

3.5.4. Conformité au standard

P.Algorithme_De_Hachage	
	Le ou les algorithmes de hachage implantés dans la TOE ne doivent pas permettre de créer deux documents produisant le même condensat. Les algorithmes seront conformes au référentiel cryptographique de la DCSSI [CRYPT-STD].

3.5.5. Interaction avec le signataire

P.Signature_De_Document (anciennement dans [PP-SIG] : O. Signature_De_Plusieurs_Documents)	
	La TOE doit permettre ~~d'enchaîner~~ la signature d'un ~~nombre fini de~~ document~~s, 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.~~ Les attributs de signature utilisés pour la signature du document doivent être ceux validés par le signataire.
Note FAST	La TOE ne permet de signer qu'un seul document à la fois.

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

P.Consentement_Explicite

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

3.5.6. Divers

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

P.Export_Signature_Electronique	
	À l'issue du processus de signature, la TOE doit transmettre au signataire la signature électronique du document au format XAdES [TS 101 903], 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 à la politique de signature appliquée *Note d'application* D'autres informations facilitant la vérification de la signature peuvent être ajoutées (ex: le certificat du signataire in extenso, un tampon d'horodatage, etc.).

P.Administration	
	La TOE doit permettre à ~~l'administrateur de sécurité~~ l'application appelante de gérer (ajouter/supprimer) les politiques de signature [B.Politique_de_signature] ~~et la table de correspondance entre les applications de visualisation et les formats de documents en entrée de la TOE [B.Correspondance_FormatDoc_Application]~~.
Note FAST	Note : Bien que ce soit l'administrateur de sécurité qui configure l'application et donc ces paramètres, c'est cette dernière qui les transmet à la TOE.

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

4. OBJECTIFS DE SECURITE

4.1. Objectifs de sécurité de la TOE

4.1.1. Objectifs généraux

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

4.1.2. Interaction avec le signataire

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

O.Consentement_Explicite	
	La TOE doit fournir au signataire les moyens d'exprimer explicitement (c'est-à-dire, de manière volontaire et non ambiguë) son consentement pour sélectionner un document ~~ou plusieurs documents~~ et déclencher le processus de signature du ~~des~~ document~~s~~ sélectionné~~s~~.
Note FAST	Dans le cadre de cette cible, l'ensemble des documents à signer est composé d'un unique document électronique au format XML. Ce document est passé en paramètre par l'application web appelante.

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

O.Document_A_Signer **(anciennement dans [PP-SIG] : O.Ensemble_De_documents_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 document, 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 validés par le signataire.

Note FAST	Dans le cadre de cette cible, l'ensemble des documents à signer est composé d'un unique document électronique au format XML.

4.1.3. Application d'une politique de signature

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

O.Validité_Du_Certificat
La TOE doit vérifier que le certificat sélectionné par le signataire est bien utilisé durant sa période de validité. *Note d'application* La référence de temps utilisée pour ce faire est la date fournie par le système d'exploitation de la machine hôte.

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

O.Export_Signature_Electronique
A l'issue du processus de signature, la TOE devra transmettre au signataire la signature électronique au format XAdES [TS 101 903], 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 à la politique de signature appliquée

4.1.4. Protection des données

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

4.1.5. Opérations cryptographiques

O.Opérations_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].

4.1.6. Contrôle de l'invariance de la sémantique du document

~~**O.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 FAST	Le type de document que signe la TOE est au format XML sous forme canonique (suivant l'algorithme C14N exclusif sans conservation de commentaire). Ce type est par nature invariant. Aucun contrôle d'invariance de sémantique n'est nécessaire.

4.1.7. Présentation du ou des documents à signer

O.Présentation_Document ~~Lancement_d'Applications_De_Présentation~~	
	La TOE devra pouvoir afficher le document à signer sous sa forme XML brut (format texte) ou sous une représentation HTML. La TOE ne devra pas permettre la signature d'un document si elle ne peut afficher le contenu du document en entier dans ces deux modes. ~~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.~~

Note FAST	~~La TOE ne devra pas permettre la signature d'un document si elle ne peut déterminer quelle application de visualisation lancer.~~
	La TOE transforme le contenu XML du document au format HTML.

4.1.8. Divers

O.Vérification_Format_Signature	
	La TOE doit s'assurer que la signature générée par le SCDev est au format PKCS #1.

4.2. Objectifs de sécurité pour l'environnement

4.2.1. Machine hôte

OE.Machine_Hôte	
	La machine hôte sur laquelle la TOE s'exécute devra être soit directement sous la responsabilité du signataire soit sous le contrôle de l'organisation à laquelle le signataire appartient, soit les deux. Le système d'exploitation de la machine hôte devra de plus offrir des contextes d'exécution séparés pour les différentes tâches qu'il exécute. Les mesures suivantes devront être appliquées : • La machine hôte est protégée contre les virus • Les échanges entre la machine hôte et d'autres machines via un réseau ouvert sont contrôlés par un pare feu contrôlant et limitant les échanges • L'accès aux fonctions d'administration de la machine hôte est restreint aux seuls administrateurs de celle-ci (différenciation compte utilisateur/administrateur) • L'installation et la mise à jour de logiciels sur la machine hôte est sous le contrôle de l'administrateur. Les moyens nécessaires au contrôle de l'intégrité de la TOE sont mis à sa disposition • Le système d'exploitation de la machine hôte refuse l'exécution d'applications téléchargées ne provenant pas de sources sûres *Note d'application* Le rôle d'administrateur de la machine hôte mentionné ci-dessus est à différencier par rapport au rôle d'administrateur de sécurité de la TOE qui a des prérogatives particulières vis-à-vis de la gestion des biens sensibles de la TOE et de ses paramètres de configuration.

4.2.2. Objectifs relatifs au SCDev et à son environnement

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

OE.Dispositif_De_Création_De_Signature	
	Le SCDev 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 o La (les) clé(s) privée(s) du signataire, protégée(s) en confidentialité et en intégrité, o Le(s) certificat(s) du signataire, protégé(s) en intégrité, à défaut une référence non ambiguë à ce(s) certificat(s), o L'association clé privée/certificat, protégée en intégrité • Biens relatifs à l'authentification du signataire o Les données d'authentification du signataire, protégées en intégrité et en confidentialité, o L'association entre des données d'authentification et le couple clé privée/certificat, protégée en intégrité.

OE.Communication_TOE/SCDev	
	L'ensemble des composants logiciels et/ou matériels assurant l'interface entre la TOE et le SCDev devra être capable de gérer (ouvrir / fermer) un canal de communication garantissant l'intégrité et l'exclusivité de la communication.
Note FAST	Dans le cadre de cette cible de sécurité un composant logiciel appelé fournisseur de services cryptographique (CSP) matérialise cette interface de communication entre la TOE et le SCDev.

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

4.2.3. Présence du signataire

OE.Présence_Du_Signataire	
	Le signataire devra être présent entre l'instant où il manifeste son intention de signer et celui ou il entre les données d'authentification permettant d'activer la clé de signature. *Note d'application* Si pour une quelconque raison, le signataire ne peut rester présent, il se doit de recommencer le processus à son début: sélection du ou des documents à signer, sélection des attributs, etc.

4.2.4. Présentation/sémantique invariante du ou des documents à signer

~~OE.Présentation_Document~~	
	~~Le système dans lequel s'insère la TOE doit posséder des applications de visualisation qui :~~ • ~~Soit retranscrivent fidèlement le type du document à vérifier,~~ • ~~Soit préviennent le signataire des éventuels problèmes d'incompatibilité du dispositif de présentation avec les caractéristiques du document.~~ ~~Dans le cas où le document à signer contient déjà des signatures, l'environnement de la TOE permettra au signataire au moins de connaître les précédents signataires, au mieux de contrôler la validité des signatures.~~
Note FAST	L'affichage du document est effectué par la TOE. De plus, dans le cadre de cette cible de sécurité le document à signer ne contient aucune signature.

4.2.5. 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.~~
Note FAST	Le type de document que signe la TOE est au format XML sous forme canonique (suivant l'algorithme C14N exclusif sans conservation de commentaire). Ce type est par nature invariant. Aucun contrôle d'invariance de sémantique n'est nécessaire.

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

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

OE.Développeur_Application_Appelante_Sûr	
	Le développeur de l'application appelante est de confiance, formé à l'utilisation de la TOE et disposant des moyens nécessaires à la réalisation de son activité.

OE.Application_Appelante_Sûre	
	L'application appelante est de confiance. L'application appelante doit être développée conformément au guide de développement (cf. § 6.2.4.2 Guide pour le développement d'applications externes). Elle s'assure en particulier de la mise sous forme canonique du document à signer, selon l'algorithme C14N exclusif sans conservation de commentaire.

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

OE.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.

OE.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 • les échanges entre la machine hôte et d'autres machines via un réseau ouvert sont contrôlés par un pare feu contrôlant et limitant les échanges • l'accès aux fonctions d'administration 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

5. EXIGENCES DE SECURITE

5.1. Exigences de sécurité fonctionnelles pour la TOE

Dans les exigences de sécurité fonctionnelles, 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.

5.1.1. 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.

5.1.1.1. 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~~**
Note FAST	Le type de document signé par la TOE est toujours invariant.

~~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: none**~~ • ~~**capability to invoke an external checker in charge of controlling that the semantics of the document to be signed is invariant**~~ • ~~**capability to inform the signer 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**.~~
Note FAST	Le type de document signé par la TOE est toujours invariant.	

~~**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.**~~ ~~*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.*~~
~~**Note FAST**~~	~~Le type de document signé par la TOE est toujours invariant.~~	
Note FAST	Le type de document signé par la TOE est toujours invariant.	

~~**FMT_MSA.3/Document 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.*~~
	~~**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.~~
~~**Note FAST**~~	Le type de document signé par la TOE est toujours invariant.	

FMT_MSA.1/Selected documents		**Management of security attributes**
	FMT_MSA.1.1/ Selected documents	
		The TSF shall enforce the **document acceptance information flow control policy** to restrict the ability to **select** the security attributes ***document's to be signed identifiers*** to **the ~~signer~~ calling application**.

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** *Raffinement global:* *The TSF shall allow the selection of documents to be signed until the signer has given his aggreement to sign.* *Note d'application*

		La liste de documents à signer ne peut plus changer à partir du moment où le signataire a donné son consentement à signer. *A noter néanmoins qu'il peut stopper le processus de signature à tout moment (voir exigence FDP_ROL.2/Abort of the signature process).*
Note FAST		La cible d'évaluation ne permet de signer qu'un seul document à la fois.

~~**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**.~~
Note FAST	Le type de document signé par la TOE est toujours invariant.	

~~**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:~~ ~~• **invoking an external module to get the status indicating whether the document's semantics is invariant or not.**~~
Note FAST	Le type de document signé par la TOE est toujours invariant.	

~~**FMT_MSA.1/ Getting 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**.~~
Note FAST	Le type de document signé par la TOE est toujours invariant.	

~~**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.**~~
Note FAST	Le type de document signé par la TOE est toujours invariant.	

5.1.2. 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 transfered to the SCDev**.	

5.1.3. Règles de validation

5.1.3.1. 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~~ calling application to change the value of signature attributes required by the applied signature policy.** *Raffinement global:* *The TSF shall allow the modification of signature attributes until the signer has given his aggreement to sign.*	

5.1.3.2. Règle 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:** o **the signer's certificate** • **operations:** o **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 the following **set of rules: none.**
FDP_IFF.1.4/Signer's certificate import	
	The TSF shall provide the following **additional capabilities**: **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 **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),** • **the private key corresponding to public key is protected by an SSCD (Application note: information available using a QCStatement, see RFC 3739)** • **the certificate is used during its validity period (Application note: the validity period is checked against the current system time and the *not Before* and *not After* dates in the certificate).** • **The certificate is issued by a trusted Certification Authority (the trusted CA list is passed to the TOE by the calling application)**

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 s**igner'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 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 DN of the signer's certificate** • **interpretation of the QCStatement** 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.**	

5.1.4. 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:**
		  o **the data to be signed formatted**
		  o **the numeric signature (once generated)**
		• **operations:**
		  o **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 and *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/Signature generation	
		The TSF shall enforce the following **set of rules: 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 display the document to the signer ~~launch the viewer corresponding to the document's format according to the document *document format/viewer association table*~~.** • **capability to activate the signing key corresponding to the selected signer's certificate.** • **send the data to be signed formatted 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**.
	Note d'application *Note that the conformance of the signer's certificate with respect to the applied signature policy is not check in the present policy but in the signer's certificate information flow control policy that is the subject of component FDP_IFC1/Signer's certificate import. In the present component the conformance of the signer's certificate is assumed established.*	

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 enforce 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** to provide **restrictive** 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**.

5.1.5. Retour de la signature electronique

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:**
	  o **the signer**
	  o **the SCDev**
	• **information:**
	  o **the generated numeric signature**
	  o **the signature attributes: document's hash, ~~reference to~~ the signer's certificate**
	• **operations:**
	  o **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:**
	  o **the signer**
	  o **the SCDev (the status of signature generation process)**

		• **information:** o **the electronic signature (the generated numeric signature, the signed document's hash, ~~the reference to~~ the signer's certificate, the reference of the applied signature policy)**
	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 **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 **additional capability :** • **Format the signature to XAdES 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	
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).**	

5.1.6. Opération cryptographiques

FCS_COP.1/Hash function	Cryptographic operation
FCS_COP.1.1/Hash function	
The TSF shall perform • **hash generation** in accordance with a specified cryptographic algorithm • **SHA-1** • **SHA-256** ~~and cryptographic key sizes [assignment: cryptographic key sizes]~~ that meet the following: **[CRYPT-STD]**, **[FIPS PUB 180-1]**, **[FIPS PUB 180-2]**. *Refinement:* *cryptographic key sizes is not applicable in the context of this hash function.*	

5.1.7. 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	

FMT_UID.1	User identification before any action
FMT_UID.2.1	
The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.	
Note FAST	Il s'agit ici de l'identification de l'application appelante utilisatrice de la TOE.

5.1.8. Administration de la TOE

5.1.8.1. 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**.~~	
Note FAST	La visualisation du document est gérée par la TOE au travers de son afficheur HTML interne (la table de correspondance permettant la transformation XML vers HMLT étant elle gérée par l'application appelante).

~~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 to manage [assignment: management operations] the document format/viewer association table.**~~	

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

5.1.8.2. 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**~~ **calling application of the TOE**. *Note d'application* *Ce composant fonctionnel doit être instancié de manière cohérente avec le composant FMT_SMF.1/Management of the signature policies.*	
Note FAST	La politique de signature est transmise par 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.** *Note d'application* *Ce composant fonctionnel doit être instancié de manière cohérente avec le composant FMT_MTD.1Management of the signature policies.*	
Note FAST	La politique de signature est transmise par l'application appelante.	

5.2. Exigences d'assurance pour la TOE

Le niveau des exigences de sécurité d'assurance est EAL2, augmenté des composants ADV_HLD.2, ALC_DVS.1, ALC_FLR.3, AVA_MSU.1, AVA_VLA.2 pour l'ensemble de la TOE et des composants ADV_LLD.1, ADV_IMP.1, ALC_TAT.1 pour les fonctions cryptographiques spécifiées au travers de la classe FCS.

Classe d'assurance	Composants d'assurance		
Gestion de configuration (ACM)	ACM_CAP	2	Capacités de la gestion de configuration
Livraison et exploitation (ADO)	ADO_DEL	1	Livraison
	ADO_IGS	1	Installation, génération et démarrage
Développement (ADV)	ADV_FSP	1	Spécifications fonctionnelles
	ADV_HLD	**2**	Conception de haut niveau
	ADV_IMP	**1**	Représentation de l'implémentation (pour la classe fonctionnelle FCS uniquement)
	ADV_LLD	**1**	Conception de bas niveau (pour la classe fonctionnelle FCS uniquement)
	ADV_RCR	1	Correspondance des représentations
Guide (AGD)	AGD_ADM	1	Guide de l'administrateur
	AGD_USR	1	Guide de l'utilisateur
Support au cycle de vie (ALC)	ALC_DVS	1	Sécurité du développement
	ALC_FLR	**3**	Correction d'anomalies
	ALC_TAT	**1**	Outils et techniques (pour la classe fonctionnelle FCS uniquement)
Tests (ATE)	ATE_COV	1	Couverture
	ATE_FUN	1	Tests fonctionnels
	ATE_IND	2	Tests indépendants
Estimation des vulnérabilités (AVA)	AVA_MSU	**1**	Utilisation impropre
	AVA_SOF	1	Résistance des fonctions de sécurité de la TOE
	AVA_VLA	**2**	Analyse de vulnérabilités

6. SPECIFICATIONS GLOBALES DE LA CIBLE D'EVALUATION

6.1. Fonction de sécurité pour la TOE

6.1.1.1. 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 au format XML sous forme canonique (conformément à l'algorithme C14N Exclusif sans conservation de commentaire [XML-C14EXC]) et encodé en UTF-8
- De la part de F.Applique_Politique_Signature :
  - référence à la politique de signature (si existante)
  - acte d'engagement
  - L'algorithme de hachage à utiliser pour générer la signature (cf §2.2.2.6)
  - 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 selon le standard XAdES encodé en UTF-8. 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, un code d'erreur (si tout ce passe correctement, le code est ST_OK) et l'url de la page web vers laquelle redirigé le signataire (qui peut aussi être une page d'échec).

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

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

6.1.1.2. F.Sélection_Certificat

Cette fonction demande au signataire de sélectionner un certificat dans la liste des certificats filtrée suivant la politique de signature. Les certificats proposés au signataire répondent aux règles suivantes :

- D'une part à la politique de signature, c'est-à-dire que la liste des certificats proposés a été filtrée suivant la politique de signature,
- Le certificat est utilisé dans sa période de validité (i.e. il n'est pas expiré)

6.1.1.3. F.Présentation_Document

La TOE présente le contenu du document au signataire :

- Soit au format XML brut (sous forme texte)
- Soit au format HTML. Dans ce format, la TOE effectue d'abord la transformation du contenu XML en HTML, en s'aidant du fichier de configuration contenant la correspondance entre les balises XML et celles HTML.

Le signataire choisit le type d'affichage : il peut basculer de l'un à l'autre.

6.1.1.4. F.Applique_Politique_Signature

Cette fonction permet à l'application appelante de définir la politique de signature, puis l'applique.

Une politique de signature est constituée de :

- Les informations caractérisant la politique de signature déterminée en fonction du rôle présumé du signataire :
    - Une description littérale de la politique de signature
    - Une URL permettant de récupérer une version complète (et signée) de la politique de signature
    - Une référence non ambiguë à la politique de signature, constituée :
        - d'un condensat la politique de signature, et de
        - l'identifiant de l'algorithme de hachage utilisé pour calculer le condensat.
- la liste des AC autorisées
- L'algorithme de hachage à utiliser pour générer la signature (cf §2.2.2.6)
- le rôle du signataire
- le lieu de signature
- le type d'engagement
- Le certificat est utilisable ou non pour des applications de non répudiation (bit 1 du paramètre KeyUsage)

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

- liste des AC 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

Cette fonction applique la politique de signature :

- Elle filtre les certificats disponibles pour le signataire en fonction des paramètres suivant :
  - les AC autorisées,
  - requiert ou non la non-répudiation,
- Et elle insère dans les attributs de signature les données de la politique de signature marquées comme telle. Ces données sont :
  - L'algorithme de hachage à utiliser pour générer la signature
  - Les informations caractérisant la politique de signature
  - Le rôle du signataire
  - La date de la signature (date de la machine hôte)
  - Le lieu de signature
  - Le type d'engagement

6.1.1.5. 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.

6.1.1.6. 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 :

- Les informations caractérisant la politique de signature déterminée en fonction du rôle présumé du signataire :
  - Une description littérale de la politique de signature
  - Une URL permettant de récupérer une version complète (et signée) de la politique de signature
  - Une référence non ambiguë à la politique de signature, constituée :
    - d'un condensat la politique de signature, et de
    - l'identifiant de l'algorithme de hachage utilisé pour calculer le condensat.
- le rôle du signataire

- les informations caractérisant le certificat de signature sélectionné par le signataire :
    - Le nom de l'autorité de certification émettrice du certificat de signature
    - Le numéro de série du certificat de signature
- Une référence non ambiguë au certificat de signature, constituée :
    - d'un condensat du certificat, et de
    - l'identifiant de l'algorithme de hachage utilisé pour calculer le condensat.
- la date et l'heure présumées de la signature déterminée par la TOE à partir de l'heure système de la machine hôte
- le lieu de signature
- le type d'engagement

6.2. Mesures d'assurance pour la TOE

Les mesures d'assurance suivantes sont nécessaires pour le niveau d'évaluation EAL2 augmenté demandé au paragraphe 5.2 :

- 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

6.2.1. Développement

6.2.1.1. 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

6.2.2. Support au développement et livraison

6.2.2.1. 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.2
- ALC_DVS.1
- ALC_TAT.1

6.2.2.2. 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

6.2.2.3. 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

6.2.3. Tests et analyse de vulnérabilité

6.2.3.1. 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.1
- ATE_FUN.1
- ATE_IND.2

6.2.3.2. 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

6.2.4. Guides

6.2.4.1. 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
- AVA_MSU.1

6.2.4.2. Guide pour le développement d'applications externes

Un guide s'adressant aux développeurs d'applications décrit la manière d'utiliser les fonctions de sécurité du produit et leurs interfaces. Une application externe sera considérée de confiance si et seulement si elle a été développée conformément à ce guide.

Ce guide stipule aussi que le guide utilisateur doit être accessible en ligne pour les signataires (cf. §6.2.4.3).

Le document fourni pour répondre à ces mesures est :

- Guide de développement d'applications

Cette mesure d'assurance couvre en partie (la seconde mesure décrite au paragraphe 6.2.4.3 permet de couvrir complètement l'exigence AGD_ADM.1) l'exigence suivante :

- AGD_ADM.1
- AVA_MSU.1

6.2.4.3. Guide pour la création de tables de correspondance XML / HTML

Ce guide indique la syntaxe du fichier de correspondance entre les balises XML et les balises HTML (à afficher).

Le document fourni pour répondre à ces mesures est :

- Guide pour la création de tables de correspondance XML / HTML

Cette mesure d'assurance couvre en partie (la seconde mesure décrite au paragraphe 6.2.4.2 permet de couvrir complètement l'exigence AGD_ADM.1) l'exigence suivante :

- AGD_ADM.1
- AVA_MSU.1

6.2.4.4. 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
- AVA_MSU.1

6.2.5. Couverture des mesures d'assurance

Composant d'assurance	Mesure d'assurance
ACM_CAP.2	§6.2.2.1
ADO_DEL.1	§6.2.2.3
ADO_IGS.1	§6.2.4.1
ADV_FSP.1	§6.2.1.1
ADV_HLD.2	§6.2.1.1
ADV_LLD.1	§6.2.1.1
ADV_IMP.1	§6.2.1.1
ADV_RCR.1	§6.2.1.1
AGD_ADM.1	§6.2.4.2 §6.2.4.3
AGD_USR.1	§6.2.4.4
ALC_DVS.1	§6.2.2.1
ALC_TAT.1	§6.2.2.1
ALC_FLR.3	§6.2.2.2
ATE_COV.1	§6.2.3.1
ATE_FUN.1	§6.2.3.1
ATE_IND.2	§6.2.3.1
AVA_MSU.1	§6.2.4.1 §6.2.4.2 §6.2.4.3 §6.2.4.4
AVA_SOF.1	-
AVA_VLA.2	§6.2.3.2

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

7. CONFORMITE A UN PROFIL DE PROTECTION

Cette section fournit les déclarations de conformité à un profil de protection.

7.1. Référence du profil de protection

La TOE est conforme au PP « Application de création de signature » [PP-SIG].

[Section à mettre à jour une fois le référencement du PP terminé]

7.2. 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 en rouge pour les ajouts et en ~~rouge barré~~ pour les suppressions.

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

7.2.1. 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 modifié et deux autres sont créés :

- L'administrateur de sécurité devient celui 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) ;
- 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 ;
- 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.

Les modifications suivantes on été apportées par rapport au profil de protection :

Catégorie	Nom de l'élément	Modification apportée
Sujet	S.Administrateur_De_Sécurité	Précision : devient celui de l'application appelante
Sujet	S.Développeur_Application_Appelante	Ajout de l'élément
Sujet	S.Application_Appelante	Ajout de l'élément
Hypothèse	H.Développeur_Application_Appelante_Sûr	Ajout de l'élément
Hypothèse	H.Application_Appelante_Sûre	Ajout de l'élément
Objectif	OE.Développeur_Application_Appelante_Sûr	Ajout de l'élément

Catégorie	Nom de l'élément	Modification apportée
Objectif	OE.Application_Appelante_Sûre	Ajout de l'élément
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_SMR.1	Modification : pour la TOE, l'administrateur est l'application appelante

7.2.2. 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, qui ne peut être que dans un unique format : le XML.

Une correspondance est faite entre les balises XML et un affichage HTML au travers d'une table de correspondance définie dans un fichier externe à la TOE.

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

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

Les modifications suivantes ont alors été apportées :

Catégorie	Nom de l'élément	Modification apportée
Bien	B.Correspondance_FormatDoc_Application	Suppression de l'élément
Hypothèse	H.Présentation_Du_Document	Suppression de l'élément puisque la TOE affiche elle-même le document
Hypothèse	H.Présentation_Signatures_Existantes	Suppression de l'élément puisque la TOE affiche elle-même le document Toutefois, il faut noter que la TOE ne permet pas la contre-signature et donc n'affiche pas les signatures déjà existantes du document.
Objectif	O.Lancement_d'Applications_De_Présentation O.Présentation_Document	O. Lancement_ d'Applications_ De_Présentation a été renommé et modifié afin de préciser que l'affichage du document est effectué par la TOE elle-même

Catégorie	Nom de l'élément	Modification apportée
Objectif	OE.Présentation_Document	Suppression de l'élément
Exigence fonctionnelle de sécurité	FDP_IFF.1/Signature generation	Précision : la TOE effectue l'affichage du document à signer
Exigence fonctionnelle de sécurité	FMT_MTD.1/Document format/viewer association table	Suppression de ces deux éléments puisque la TOE ne signe qu'un format de document et l'affiche
Exigence fonctionnelle de sécurité	FMT_SMF.1/Management of the document/format association table	

7.2.3. 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 signe des documents au format XML, préalablement mis sous forme canonique, par l'application appelante, suivant l'algorithme C14N exclusif, dans sa variante sans conservation des commentaires. La sémantique de ce type de document étant stable par nature, aucun contrôle de sémantique sur le document n'est nécessaire.

Les éléments du profil de protection concernant le contrôle de sémantique n'ont donc pas été reportés :

Catégorie	Nom de l'élément	Modification apportée
Hypothèse	H.Contrôle_Invariance_Sémantique_Document	Suppression de l'élément
OSP	P.Sémantique_Document_Invariante	Suppression de l'élément
Objectif	O.Contrôle_Invariance_Document	Suppression de l'élément
Objectif	OE.Contrôle_Sémantique_Document_Signé	Suppression de l'élément
Exigence fonctionnelle de sécurité	FDP_IFC.1/Document acceptance	Suppression de l'élément
Exigence fonctionnelle de sécurité	FDP_IFF.1/Document acceptance	Suppression de l'élément
Exigence fonctionnelle de sécurité	FDP_ITC.1/Document acceptance	Suppression de l'élément
Exigence fonctionnelle	FMT_MSA.3/Document acceptance	Suppression de l'élément

Catégorie	Nom de l'élément	Modification apportée
de sécurité		
Exigence fonctionnelle de sécurité	FMT_MSA.1/Document's semantics invariance status	Suppression de l'élément
Exigence fonctionnelle de sécurité	FMT_SMF.1/Getting document's semantics invariance status	Suppression de l'élément
Exigence fonctionnelle de sécurité	FMT_MSA.1/ Getting signer agreement to sign an instable document	Suppression de l'élément
Exigence fonctionnelle de sécurité	FMT_SMF.1/Getting signer agreement to sign an instable document	Suppression de l'élément
Exigence fonctionnelle de sécurité	FDP_IFF.1/Signature generation	Suppression de l'attribut du sujet concernant l'accord de signer un document instable

7.2.4. Signature au format XAdES

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

Catégorie	Nom de l'élément	Modification apportée
Bien	B.Signature_Electronique	Précision sur le format de la signature
OSP	P.Export_Signature_Electronique	Précision sur le format de la signature
Objectif	O.Export_Signature_Electronique	Précision sur le format de la signature
Exigence fonctionnelle de sécurité	FDP_IFF.1/Electronic signature export	Raffinement (ajout de la capacité à formater la signature au format XAdES)

7.2.5. 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
OSP	P. Vérification_Format_Signature	Ajout de l'élément
Objectif	O.Vérification_Format_Signature	Ajout de l'élément pour couvrir l'OSP
Exigence fonctionnelle de sécurité	FDP_IFF.1/Electronic signature export	Ajout de la capacité à vérifier que la signature générée est au format PKCS #1

7.2.6. 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
Sujet	S.Signataire	Précision sur la politique de signature : elle est définie par l'application appelante
Sujet	S.Application_Appelante	Ajout du sujet qui transmets à la TOE la politique de signature
OSP	P.Administration	Précision sur la gestion des politiques de signature : l'application appelante définit la politique de signature au travers d'un paramètre d'entrée
Objectif	O.Administration	Cf ci-dessus
Objectif	OE.Authenticité_Origine_Politique_Signature	Précision sur l'administrateur : remplacement du mot *TOE* par *application appelante.*
Exigence fonctionnelle de sécurité	FMT_MTD.1/Management of the signature policies	Assignement : operation possible : *define*
		Précision : c'est l'application appelante transmit la politique de signature à la TOE
Exigence fonctionnelle de sécurité	FMT_SMF.1/Management of the signature policies	Assignement : operation possible : *define*

7.2.7. Signature d'un seul document

La TOE ne permet de signer qu'un document à la fois. Bien qu'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
Bien	B.Ensemble_Des_Documents_A_Signer	Renommé en B.Document_A_Signer
		Précision : la TOE signe un seul document à la fois
Sujet	S.Signataire	Précision : la TOE signe un seul document à la fois

Catégorie	Nom de l'élément	Modification apportée
OSP	P.Signature_De_Document	Modification de l'intitulé (anciennement P.Signature_De_ Plusieurs_Document) Précision : la TOE signe un seul document à la fois
Objectif	O.Documents_A_Signer	Modification de l'intitulé (anciennement O. Ensemble_De_ Documents_A_Signer) Précision : la TOE signe un seul document à la fois
Objectif	O.Consentement_Explicite	Précision : la TOE signe un seul document à la fois
Exigence fonctionnelle de sécurité	FMT_SMF.1/Selection of a list of documents	Précision : la TOE signe un seul document à la fois

7.2.8. Autres assignements

Les *assignements* suivants demandés par le profil de protection ont été effectués :

Catégorie	Nom de l'élément	Modification apportée
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_ITC.1/Explicit signer agreement	Assignement : description des actions à effectuer par le signataire pour donner son consentement explicite à signer un document
Exigence fonctionnelle de sécurité	FCS_COP.1/Hash function	Assignement : algorithme de hachage

7.2.9. Autres raffinements

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

Catégorie	Nom de l'élément	Modification apportée
Exigence fonctionnelle de sécurité	FDP_IFF.1/Signature generation	Raffinement : la TOE doit avoir la capacité de transférer les données à signer et de recevoir la signature de la part du SCDev

7.2.10. Autres biens

Concernant les 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	D.Données_A_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)	-

8. ARGUMENTAIRE

L’argumentaire n’est pas disponible dans la version publique de ce document.