Dictao
152, avenue de Malakoff
75116 Paris

Cible de sécurité (version publique)

Dictao Validation Server (DVS)

Date de dernière mise à jour :
16 octobre 2007 Référence : dictao_adovi_cibledesecurite_publique

Références du document

Référence : dictao_adovi_cibledesecurite_publique.doc
Date de dernière mise à jour : 16 octobre 2007
Version : 1.0
Version du logiciel associé : 4.0.6

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

Diffusion : PUBLIQUE

Rédaction (nom): **Dictao**	**Vérification (nom(s)) :** **Dictao**	**Validation (nom) :** **Dictao**

SOMMAIRE

1. ACRONYMES ET ABREVIATIONS

1.1 Abréviations

AC	Autorité de certification
CRL	*Certificate Revocation List* (Liste de Révocation de Certificat – LCR)
DN	*Distinguish Name* (Nom du certificat)
DVS	*Dictao Validation Server*
HSM	*Hardware Security Module* (Module de sécurité matériel)
IGC	Infrastructure de Gestion de Clés
JVM	*Java Virtual Machine*
OCSP	*Online Certificate Status Protocol* (Protocole de statut des certificats)
OID	*Object Identifer*
SCDev	*Signature Creation Device* (Dispositif de création de signature)
SSCD	*Secure Signature Creation Device* (Dispositif Sécurisé de Création de Signature)
ST	*Security Target* (Cible de sécurité)
TOE	*Target Of Evaluation* (Cible d'évaluation)
XAdES	*XML Advanced Electronic Signature*

1.2 Terminologie

Super-Administrateur	Personne autorisée à accéder à l'interface de super-administration de DVS
Administrateur	Personne autorisée à accéder à l'interface d'administration de DVS
Gestionnaire	Personne autorisée à accéder à l'interface de suivi de gestion de DVS
Application cliente	Application cliente du service de validation DVS
Interface d'appel	Partie logicielle devant être intégrée à une application pour qu'elle puisse envoyer des requêtes à DVS
Opérateur d'hébergement	Personne autorisée à accéder aux machines. On parle aussi d'opérateur (de la machine hébergeant DVS).
Utilisateur	Administrateur, super-administrateur, gestionnaire ou super-gestionnaire de DVS
Utilisateur Final	Utilisateur de l'application cliente de DVS

1.3 Références

Référence	Document
[CC]	Critères Communs : • *Common Criteria for Information Technology Security Evaluation, Part 1:* *Introduction and general model.* référence CCMB-2005-08-001 Version 2.3 August 2005 • *Common Criteria for Information Technology Security Evaluation, Part 2:* *Security functional requirements*. référence CCMB-2005-08-002 Version 2.3 August 2005 • *Common Criteria for Information Technology Security Evaluation, Part 3:* *Security Assurance Requirements.* référence CCMB-2005-08-003 Version 2.3 August 2005
[CEM]	*Common Methodology for Information Technology Security Evaluation, Evaluation Methodology* référence CCMB-2004-08-004 Version 2.3 August 2005
[CMS]	*Cryptographic Message Syntax (CMS)* *Request For Comments RFC 3852* Juillet 2004
[CRYPT_STD]	*Mécanismes cryptographiques - Règles et recommandation concernant le choix et dimensionnement des mécanismes cryptographiques de niveau de robustesse* standard *et* renforcé Référence 001064/SGDN/DCSSI/DSD/AsTec Version 1.0 mai 2004 DCSSI
[EXT_DCSSI_PP]	*Profil de protection « Module de vérification de signature électronique »* référence PP-MVSE (DCSSI PP/nc0503) version 1.0 février 2005
[EXT_TS_101_733]	*Electronic signature formats* version 1.5.1 15 décembre 2003 ETSI standard
[FIPS 180-2]	*Secure Hash Standard* (+ Change Notice to include SHA-224) Federal Information Processing Standards (FIPS) Publication 180-2 February 2004

Référence	Document
[PKCS #1]	*PKCS #1 – RSA Cryptography Standard* Version 2.1 June 2002 RSA Laboratories
[PKCS #7]	*PKCS #7 – RSA Cryptography Standard* Version 1.5 Novembre 1993 RSA Laboratories
[PKCS #11]	*PKCS #11 – RSA Cryptography Standard* Version 2.0 April 1997 RSA Laboratories
[PKCS #12]	*PKCS #12 – RSA Cryptography Standard* Version 1.0 June 1999 RSA Laboratories
[PRIS v2]	*Politique de Référencement InterSectorielle* version 2.0 http://www.adae.gouv.fr/ juillet 2005
[QUA_STD]	*Processus de qualification d'un produit de sécurité – Niveau standard.* référence 001591/SGDN/DCSSI/SDR Version 1.0 juillet 2003 DCSSI
[RFC 3280]	*RFC 3280* http://www.faqs.org/rfcs/rfc3280.html
[RFC 3739]	*RFC 3739* http://www.faqs.org/rfcs/rfc3739.html
[XAdES]	*XML Advanced Electronic Signatures* référence ETSI TS 101 903 version 1.2.2 et 1.3.2
[ST]	*Cible de sécurité* Projet ADOVI Référence dictao_adovi_cibledesecurite version 7.0

2. INTRODUCTION

2.1 Identification de la cible de sécurité

Ce document constitue la version publique de la cible de sécurité de DVS « Dictao Validation Server ».

- Auteur : **Dictao**
- Titre de la ST : **Dictao Validation Server (DVS) – Cible de sécurité (version publique)**
- Version du document : **1.0**
- Identifiant de la TOE : **DVS**
- Version de la TOE : **4.0.6**
- Plateforme : **la plateforme sur laquelle la TOE est évaluée est identifiée au paragraphe 3.3.1**
- Mots clé : **Signature électronique, Application de vérification de certificat, Application de vérification de signature électronique, Serveur**

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

- Titre de la ST : **Dictao Validation Server (DVS) – Cible de sécurité**
- Version du document : **7.0**
- Référence : **dictao_adovi_cibledesecurite**

2.2 Vue d'ensemble de la cible de sécurité

2.2.1 Définition de la cible d'évaluation

La cible d'évaluation définie dans le présent document est constituée d'une application serveur de validation de signature électronique et de certificat.

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

Nom de l'objet : Dictao Validation Server (DVS)

Numéro de la version évaluée : 4.0.6

2.2.2 Conformité aux Critères Communs

Conformité aux CC

La présente cible de sécurité est conforme à la partie 2 des Critères Communs étendue des composants FDP_MRU.1 (voir §9.2) et FPT_TDI.1 (voir §9.3) et à la partie 3 des Critères Communs, Version 2.3 avec interprétations. Les interprétations applicables à la présente évaluation sont :

- RI # 86 – Role of Sponsor ;
- RI # 137 – Rules governing binding should be specifiable ;
- RI # 146 – C&P elements include characteristics ;
- RI # 192 – Sequencing of sub-activities ;
- RI # 220 – FCS_CKM/COP dependency on FDP_ITC.1 ;
- RI # 227 – CC Part2 F.12 user notes ;

- RI # 228 – Inconsistency between FDP_ITC and FDP_ETC ;
- RI # 232 – FDP_ROL statement ;
- RI # 243 – Must Test Setup And Cleanup Code Run Unprivileged.

Conformité à un PP

La cible de sécurité est conforme au profil de protection « Module de vérification de signature électronique » [EXT_DCSSI_PP].

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

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

Niveau d'assurance

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

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

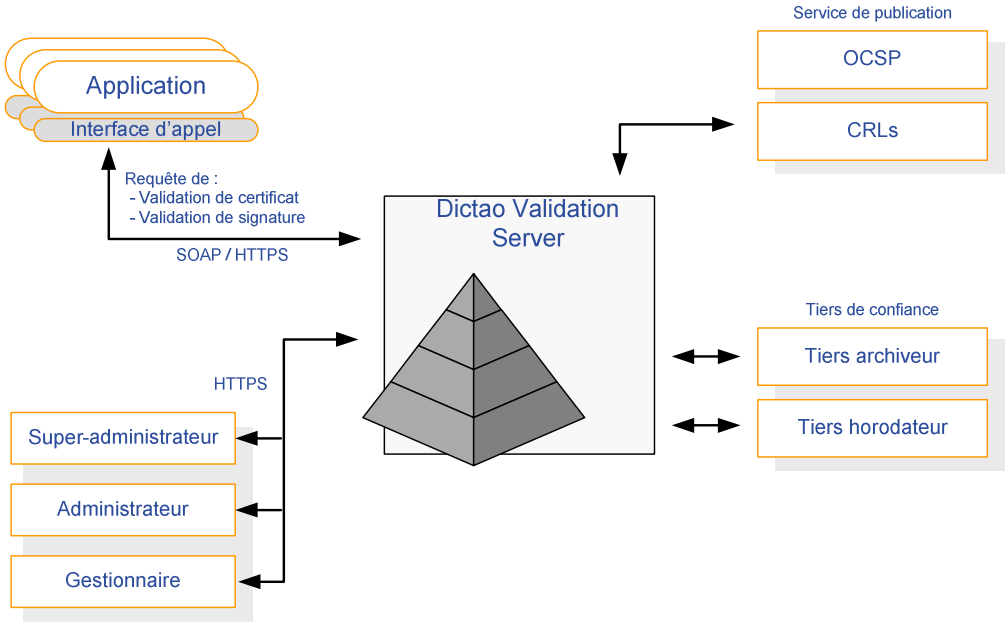
Niveau de résistance

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

2.2.3 Principe général de fonctionnement

DVS est un serveur de validation de certificats et de signatures électroniques multi-applications supportant les standards de signature courants : PKCS #7, CMS, PDF, XML-DSig et XAdES.

Ce serveur permet aux applications souhaitant intégrer des fonctionnalités de confiance telles que l'authentification par certificat ou la signature de documents électroniques, de déléguer toute la complexité du système de confiance à un service unique facilement configurable et qui saura répondre à la quasi-totalité des « cinématiques de confiance » des organisations. L'application appellera très simplement les services du serveur de validation en utilisant le protocole *SOAP* ou *WebService*.



* Uniquement pour les fonctions cryptographiques spécifiées au travers des exigences de la classe FCS au paragraphe 6.1.7.6.

Les fonctions premières du serveur de validation sont :

- La **validation de certificat** : « authenticité » du certificat, « reconstitution de la chaîne de validation », consultation des listes de révocation (dans une approche multi-AC). Cette fonction permet de garantir l'authentification de l'acteur (signature, contrôle d'accès…)
- La **validation de signature** : validation de l'intégrité du message et de la non-répudiation.
- La **constitution de preuve :** horodatage, signature et archivage de la preuve

2.2.4 Exemples d'utilisation

DVS peut être utilisé pour deux fonctions majeures :

➢ **La validation du certificat pour une gestion de l'identité ou une fonction de contrôle d'accès**

Une application reçoit un certificat d'authentification et souhaite vérifier la validité de ce certificat selon des critères prédéfinis :

- L'application envoie le certificat à valider à DVS. Le canal est sécurisé, les informations sont chiffrées et toute modification est détectée.
- DVS vérifie le certificat selon la politique de validation souhaitée par l'application (horodatage, type du certificat, autorités de certifications autorisées…) et renvoie la réponse à l'application.
- Par ailleurs, DVS archive une copie **signée** et **horodatée** de tous les éléments de la requête ainsi que la réponse et les éléments permettant d'effectuer une vérification « manuelle », *a posteriori*, des vérifications effectuées par la TOE, par exemple, en cas de litige ou à des fins de diagnostic d'erreur.
  Cet archivage est local (via une base de données directement connectée à DVS) ou effectué par un tiers.

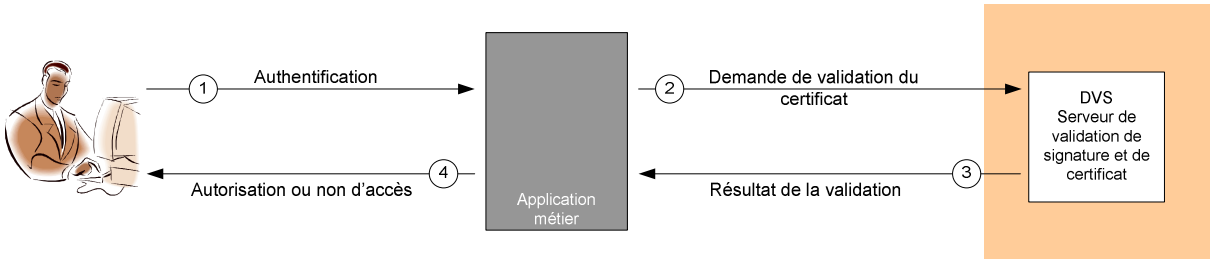


Figure 1 - Exemple d'utilisation en contrôle d'accès

➢ **La validation d'une signature**

Une application reçoit une transaction signée (ordre de virement, contrat, demande d'intervention en maintenance…), et souhaite vérifier la validité de cette signature selon des critères prédéfinis.

- L'application transmet la signature à DVS. Le canal est sécurisé, les informations sont chiffrées et toute modification est détectée.
- DVS vérifie la signature ainsi que le certificat inclus en utilisant la politique de validation souhaitée par l'application, puis renvoie la réponse à l'application. Cette réponse est signée par DVS.
- DVS archive une copie **signée** et **horodatée** de tous les éléments de la requête, ainsi que la réponse, et les éléments permettant d'effectuer une vérification *a posteriori*. Si nécessaire, des informations de facturation du service pourront aussi être produites.

Cet archivage est local (au travers d'une base de données directement connectée à DVS) ou effectué par un tiers.

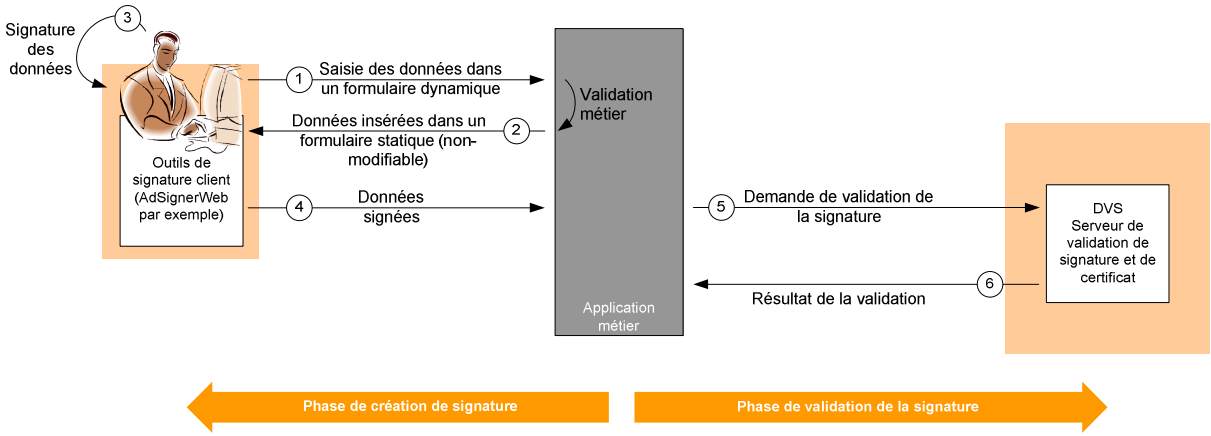


Figure 2 - Exemples d'utilisation en validation de signature

2.2.5 Présentation de la cible de sécurité

La cible de sécurité définit les bases pour l'évaluation de DVS. Elle est organisée comme suit :

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

3. DESCRIPTION DE LA CIBLE D'EVALUATION (TOE)

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

3.1 Description générale

La cible d'évaluation (ou TOE – *Target Of Evaluation*) est une partie de *Dictao Validation Server* (DVS). Le serveur DVS permet de valider un certificat ou une signature électronique, générant une preuve pour chaque requête de validation. La partie du serveur non évaluée correspond à des fonctionnalités non critiques en termes de sécurité et de service.

La TOE est utilisée par une application cliente, qui envoie une requête demandant la validation d'un certificat ou de la signature d'un document. La TOE prend en charge les signatures multiples (co-signature et contre-signature).

Les contrôles effectués par la TOE lors d'une validation de signature électronique sont définis au sein d'une Politique de Confiance DVS. Cette Politique de Confiance, paramétrée par un administrateur, est sélectionnée par l'application appelante lors de l'appel à la TOE. Elle contient en particulier les éléments de la politique de signature qui doit être appliquée.

La politique de signature définie dans une politique de confiance DVS est à distinguer de la politique de signature qu'applique la TOE lorsqu'elle crée la signature de la preuve de validation.

Nous parlerons dans la suite du document de :

- **Politique de signature** pour désigner une politique de signature que la TOE applique lorsqu'elle valide une signature.
- **Politique de signature de preuve**, pour désigner une politique de signature utilisée lors de la génération d'une preuve de validation.

3.1.1 Groupes et rôles

DVS permet de définir un certain nombre de groupes dans l'idée d'avoir plusieurs domaines applicatifs distincts. À chaque groupe sont associés :

- Un ou plusieurs administrateurs de sécurité (« *administrators* »), aussi appelés « administrateurs » tout court
- Un ou plusieurs gestionnaires (« *operators* »)
- Une ou plusieurs applications
- Une ou plusieurs politiques de confiance

Les administrateurs d'un groupe définissent les autres rôles et paramètres du groupe (identité des gestionnaires, ajout et suppression d'administrateurs du groupe, applications autorisées et politiques de confiance). Les gestionnaires de groupe consultent les preuves de validation générées par les requêtes (transactions) des applications clientes, à des fin d'audit du groupe.

Les groupes et leurs administrateurs initiaux sont eux-mêmes gérés par le ou les super-administrateurs (« *super-administrator* »). Enfin, il existe un rôle de super-gestionnaire (« super-operator »), qui peut consulter les preuves de validation de tous les groupes.

Les super-administrateurs sont de plus chargés de configurer certains paramètres techniques du serveur, comme les clés de signature (affectation d'une clé à un groupe), les autorités de certification du serveur, les paramètres de connexion aux éventuels serveurs OCSP, d'horodatage, etc.

3.1.2 Politiques de Confiance DVS

Pour chaque application cliente enregistrée, l'administrateur définit un certain nombre de transactions et associe à chacune d'entre elles une politique de confiance (PC). Cette correspondance entre transaction et politique de confiance est définie en accord avec le promoteur de l'application cliente.

Une Politique de Confiance DVS définit :

- Le niveau de confiance attendu (qualifié ou non)
- La taille maximale de la requête de validation
- Les paramètres de validation de la signature (3.1.2.1)
- Les paramètres de validation du certificat de signature (3.1.2.2)
- Les paramètres de constitution et de conservation de la preuve (3.1.2.3)

Un administrateur peut créer, modifier, effacer autant de politiques de confiance qu'il le souhaite. La création, modification ou suppression d'une PC se fait via l'interface d'administration de DVS. Cette interface permet à l'administrateur de configurer tous les paramètres de la politique.

3.1.2.1 Paramètres de validation de la signature

Les paramètres de validation de la signature précisent :

- Le format de signature attendu (XML-DSig, XAdES, PKCS #7, CMS ou PDF)
- Le serveur d'horodatage à utiliser pour effectuer l'horodatage de réception de la signature
- Les propriétés de signature autorisées :
  - Rôles pouvant être endossés par le signataire
  - Lieux de signature autorisés (comprenant la ville, le code postal et le pays)
  - Documents organisationnels décrivant les politiques de signature autorisées. Chacun de ces documents est identifié de façon non ambiguë par son OID et son empreinte.
  - Types d'engagements autorisés (preuve d'origine, de réception, de remise, d'émission ou d'approbation)
- Les éléments nécessaires au contrôle un jeton d'horodatage si un tel jeton est présent dans la signature à valider
- Si la stabilité sémantique du document signé doit être contrôlée ou non, en fonction des formats. Ainsi, on peut décider de contrôler la stabilité des documents HTML mais pas celle d'autres formats.
  DVS ne permet de vérifier que les formats supportés par le module de contrôle sémantique (3.2.12) : les administrateurs ne peuvent imposer de vérifier que les formats supportés par ce module.
- La liste des applications de visualisation de référence pour les documents signés.

3.1.2.2 Paramètres de validation du certificat

Les paramètres de validation du certificat de signature :

- Liste des autorités de certification autorisées, et pour chacune de ces autorités, méthode à appliquer pour vérifier le statut du certificat (par consultation des listes de certificats révoqués ou par interrogation en temps réel d'un serveur OCSP)
- Liste blanche des certificats explicitement autorisés
- Liste blanche des DN de certificats explicitement autorisés

- Contraintes sur les extensions du certificat :
  - Liste des politiques de certification autorisées, identifiées de façon non ambiguë par leurs OID.
  - Liste des usages de la clé autorisés. Parmi ces *keyUsage* on trouve en particulier celui relatif à la non-répudiation.
  - Un paramètre indiquant si le certificat doit être qualifié ou non
  - Un paramètre indiquant si la clé privée associée au certificat doit être protégée par un SSCD

3.1.2.3 Paramètres de constitution de la preuve de validation

Les paramètres de constitution de la preuve :

- Insertion des références aux données de validation
- Insertion des valeurs des données de validation
- Politique de signature de preuve à appliquer pour signer la preuve

3.1.3 Formats de signature

Les formats de signature suivants sont pris en charge par la TOE :

- **Formats de signature XML :**
  - **XML-DSig :** signatures respectant les spécifications **XML-DSig** (XML Digital Signature) définies par le W3C : www.w3.org/2000/09/xmldsig
  - **XAdES :** signature respectant le format **standard européen XAdES** (XML Advanced Electronic Signature) de l'ETSI (www.etsi.org) qui définit un jeu d'extensions complémentaires par rapport au format XML-DSig. Ces extensions visent en particulier à assurer le maintien de la validité des signatures dans le temps. Pour des raisons d'interopérabilité avec d'autres solutions, nous supportons les trois versions publiées de ce format, à savoir 1.2.2 et 1.3.2.
  - **Modes de signature XML supportés :**
    - **XML Enveloppée :** dans ce cas la signature XML générée est insérée dans le document lui-même ; c'est la raison pour laquelle seuls des documents au format XML peuvent être signés suivant cette méthode. Ce mode de signature est ainsi parfaitement adapté à la signature de données métier au format XML : en effet, la signature du document ne modifiant pas la structure globale du document, le traitement des autres éléments du formulaire par les applications métier n'est pas impacté par l'ajout de la signature.
    - **XML Enveloppante :** dans ce cas la signature XML générée contient le document signé : cette méthode permet de signer des documents de tout format (le document est « enveloppé » à l'intérieur de la signature) : Office, PDF, des dessins CFAO, des images, etc.
  - **Algorithmes cryptographiques supportés :**
    - Algorithmes de signature supportés :
      - RSA avec SHA-512
      - RSA avec SHA-384
      - RSA avec SHA-256 (recommandé)

- http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
- RSA avec SHA-1
  - http://www.w3.org/2000/09/xmldsig#rsa-sha1
- Tailles de clés : RSA 1024, 1536, 2048, 3072, 4096 ou 8192 bits

Algorithmes de mise sous forme canonique supportés :

Canonicalisation XML
http://www.w3.org/TR/xml-c14n
Canonicalisation XML avec commentaires
http://www.w3.org/TR/xml-c14n#WithComments
Canonicalisation XML **exclusive**
http://www.w3.org/2001/10/xml-exc-c14n#
Canonicalisation XML exclusive avec commentaires
http://www.w3.org/2001/10/xml-exc-c14n#WithComments

- **Formats de signatures binaires :**
  - **PKCS #7 / CMS :** signatures respectant les spécifications des formats binaires **PKCS #7** et **CMS**.
  - **PDF :** il s'agit du format de signature propriétaire PDF. La signature est directement embarquée dans le document PDF.
  - **Modes de signature :**
    - **Enveloppante :** dans ce cas la signature binaire générée contient le document signé : cette méthode permet de signer des documents de tout format (le document est « enveloppé » à l'intérieur de la signature) : Office, PDF, des dessins CFAO, des images, etc.
    - **Détachée :** dans ce cas la signature binaire générée est un fichier distinct du document signé. Cette méthode permet elle aussi de signer des documents de tout format.
    - **Embarquée :** uniquement dans le cas PDF (voir ci-dessus)
  - **Algorithmes cryptographiques mis en œuvre :**
    - Algorithmes de signature supportés :
      - RSA avec SHA-512
      - RSA avec SHA-384
      - RSA avec SHA-256 (recommandé)
      - RSA avec SHA-1
    - Tailles de clés : RSA 1024, 1536, 2048, 3072, 4096 ou 8192 bits

DVS gère des cinématiques de validation multiples mettant en œuvre des ***co-signatures*** (ex. : signature d'un contrat par deux parties) et des ***contre-signatures*** (ex. : signature d'un document déjà signé par un « approbateur »).

3.1.4 Vérification immédiate et vérification ultérieure

Le profil de protection sur le module de vérification de signature électronique [EXT _DCSSI_PP] envisage deux cas d'utilisation : la vérification dite immédiate et la vérification dite ultérieure.

DVS prend en charge la vérification immédiate de signature. La TOE procède à une validation de la signature électronique et constitue une preuve de validation contenant en particulier le jeton d'horodatage de réception de la signature et les données de validation utilisées. Cette preuve est signée et horodatée par la TOE avant d'être retournée à l'application appelante.

La vérification ultérieure, consistant en un rejeu de la validation de signature en utilisant les données de validation collectées lors de la vérification immédiate (et contenues dans la preuve), n'est pas prise en charge par la TOE. Cette dernière ne sait pas rejouer une preuve en exploitant les données contenues dans celle-ci.

3.2 Périmètre et architecture de la cible d'évaluation

La figure suivante donne une représentation de la cible d'évaluation et des composants essentiels à son fonctionnement mais hors périmètre d'évaluation (identifiés au paragraphe 3.3.1). Ces derniers sont une plate-forme matérielle et un système d'exploitation (non représentés) ainsi que le serveur web, un *proxy* et un HSM :

- Le serveur web gère l'interface web entre le réseau externe et la TOE. Il est indispensable au bon fonctionnement de la TOE. Chaque utilisateur (quel qu'il soit) s'authentifie auprès du serveur et le serveur auprès de l'utilisateur au travers d'une authentification mutuelle à l'aide de certificats propre à chacun des acteurs (application cliente, administrateur, gestionnaire). Le certificat d'authentification SSL du serveur est stocké et géré par le serveur web.
- Le *proxy* n'est pas nécessaire. Il dépend de la configuration du réseau dans lequel vient s'insérer la TOE.
- Le boîtier cryptographique matériel HSM permet de stocker de façon sécurisée les clés de signature de la TOE. Cela s'applique aux clés de signature de la configuration, des pistes d'audit, et des preuves de validation.
  L'utilisation de ce boîtier est optionnelle, mais sa mise en œuvre est recommandée. En son absence, la TOE rend possible le stockage de ces clés sous la forme de fichier protégés au format PKCS #12 et stockés dans la base de donnée interne de la TOE.
  Ce type de stockage est utilisé pour les clés d'authentification SSL « client » auprès des services tiers (horodatage, OCSP).

D'autres composants sont hors périmètre d'évaluation, car non critiques : le module de purge et le module d'archivage externe.

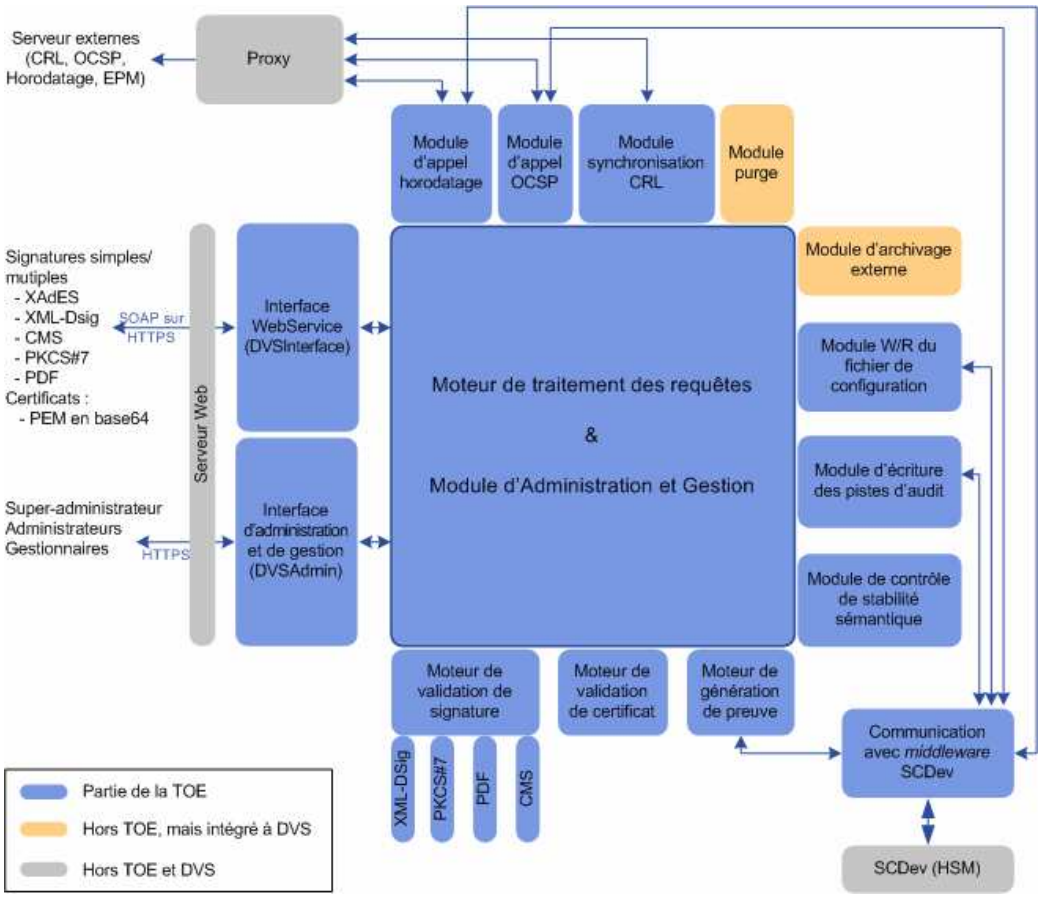


Figure 3 - Architecture du serveur de validation Dictao Validation Server

3.2.1 Interface d'utilisation « Web Services »

Cette interface gère l'interaction de la TOE avec les applications clientes. Elle se présente sous la forme d'un « *web-service* » appelable au travers d'une interface programmatique (API).

Cette interface met à disposition des applications deux services : le service de vérification de signature et le service de vérification de certificat. Elle permet en particulier :

- À l'application appelante de transmettre à la TOE
  - Le document et sa signature
  - La politique de confiance (dont fait partie la politique de signature à appliquer) sous forme d'une ID de transaction configurée dans la TOE
- À la TOE de communiquer à l'application appelante :
  - Le statut d'exécution à la fin de la validation
  - La preuve signée par DVS reprenant les éléments vérifiés, le statut d'exécution de la vérification, ainsi que les données de validation.

3.2.2 Interfaces d'administration et de gestion

3.2.2.1 Interface de super-administration

Cette interface permet aux super-administrateurs de la TOE d'effectuer des opérations de :

- Gestion des groupes d'administration et de gestion d'applications

- Gestion des administrateurs et gestionnaires
- Définition des ressources mises à la disposition des administrateurs d'applications :
  - Paramétrage des clés de signature
  - Référencement des autorités de certification
  - Référencement des politiques de certification
  - Paramétrage des serveurs d'horodatage et OCSP
  - Configuration de services d'archivage externes
- Consultation des pistes d'audit du serveur de validation

3.2.2.2 Interface d'administration

Cette interface permet aux administrateurs d'effectuer des opérations de :

- Gestion des utilisateurs au sein de leur groupe
- Paramétrage des Politiques de Confiance mutualisées
- Gestion des applications métiers
- Création de transactions pour une application donnée et association à chacune de ces transactions d'une Politique de Confiance
- Consultation des pistes d'audit relatives à leurs groupes respectifs.

3.2.2.3 Interface de gestion

Cette interface permet aux gestionnaires de groupes d'effectuer les opérations suivantes :

- Aux super-gestionnaires, d'effectuer des opérations de :
  - Recherche d'une transaction
  - Récupération d'une preuve
  - Consultation des rapports d'activité
- Aux gestionnaires de groupes, d'effectuer les mêmes opérations, mais avec un périmètre restreint aux applications du groupe dont ils sont membres.

3.2.2.4 Principe général de fonctionnement des interfaces de (super)-administration et de gestion

L'ensemble des communications entre l'utilisateur et DVS est sécurisé en termes de confidentialité et d'intégrité des échanges.

Lors de la connexion d'un utilisateur à la TOE, le certificat électronique utilisé par ce dernier lors de son authentification forte auprès du serveur web est validé par DVS, qui constitue et conserve une preuve de cette validation.

Lorsqu'un administrateur effectue une modification de configuration au travers de l'interface adéquate, un composant client léger signé est téléchargé sur son poste afin de lui permettre de signer les éléments de configuration modifiés en utilisant, en local sur son poste, sa propre clé privée.

Le fichier de configuration est ensuite transmis à DVS qui en vérifie la signature avant de prendre en compte les modifications.

3.2.3 Moteur de validation de signature

Ce moteur permet de vérifier une signature électronique.

Il commence par détecter le format de signature CMS/PKCS #7 ou XMLDSig ou XAdES ou PDF. En fonction du format, la signature est traitée par le sous-module correspondant gérant le format de signature utilisé.

Le traitement effectué par chaque sous-module est identique, seule l'interprétation du format de la signature est différente.

Le moteur applique ensuite la Politique de Confiance :

- Sélection du format de signature à partir de la valeur paramétrée dans la politique de confiance (dans le cas de l'utilisation en mode « non qualifié », la sélection du format peut se faire automatiquement, si aucun format de signature n'a été paramétré dans la politique de confiance) :
  - XML (XML-DSig, XAdES) enveloppantes ou enveloppées (avec éventuellement horodatage et signatures multiples)
  - Binaire (CMS, PKCS #7) enveloppantes ou détachées (avec éventuellement horodatage et signatures multiples)
  - PDF embarquée (signature simple uniquement)
- Horodatage de réception afin de fixer la signature dans le temps.
- Vérification cryptographique de la signature (vérification PKCS #1).
- Extraction du document signé et contrôle de sa stabilité sémantique.
- Vérification de la conformité des propriétés de la signature par rapport aux éléments paramétrés dans la Politique de Confiance
- Validation du jeton d'horodatage présent dans la signature reçue.
- Validation des certificats de signature.
- Création et scellement de la preuve de validation.

3.2.4 Moteur de validation de certificat

Le processus de la validation d'un certificat se déroule en plusieurs phases, en fonction du paramétrage de la politique de confiance :

- Contrôle d'appartenance à une liste blanche de certificats
- Contrôle d'appartenance à une liste blanche de DN
- Construction et validation de la chaîne de certification
- Vérification des extensions du certificat

➢ Phase 1 : Contrôle d'appartenance à une liste blanche de certificats

Il s'agit ici de consulter la liste blanche de certificats paramétrée dans la politique de confiance pour vérifier si le certificat est ou non présent :

- S'il est présent dans la liste, la validation passe directement à la phase 4
- Sinon, la validation se poursuit avec la phase 2.

➢ Phase 2 : Contrôle d'appartenance à une liste blanche de DN

Il s'agit ici de consulter la liste blanche de DN paramétrée dans la politique de confiance pour s'assurer que le DN du certificat correspondant à l'un des DN de la liste.

- S'il est présent la validation se poursuit avec la phase 3,
- Sinon, le certificat est marqué invalide et le processus se termine.

➢ **Phase 3 : Construction et validation de la chaîne de certification**

L'algorithme de construction de la chaîne de certification se base sur celui défini dans la RFC 3280, en ne prenant pas en compte les contraintes de nommage et de politiques.

Construction de la chaîne de certification, en remontant, à partir du certificat à valider et jusqu'au certificat de l'AC racine, la chaîne des certificats d'AC intermédiaires. Les autorités de certification de confiance sont paramétrées dans la politique de validation. Lors de la construction de la chaîne, si une même clé publique fait l'objet de deux certificats, signés par deux autorités différentes, DVS retient une chaîne de certification contenant une AC définie comme ancre de confiance.

Validation de la chaîne de certification :

- Validation du certificat de l'AC racine débutant la chaîne de certification.
- Vérification des certificats de l'AC ancre de confiance et des certificats d'AC intermédiaires.
- Vérification du certificat d'entité final.

➢ **Phase 4 : Vérification des extensions du certificat**

Il s'agit ici de s'assurer, en fonction du paramétrage effectué au niveau de la politique de confiance, que :

- Les types d'utilisation de la clé autorisés par l'AC émettrice du certificat contiennent bien les types d'utilisations exigés
- Le certificat est un certificat qualifié
- La clé privée associée au certificat est protégée par un SSCD (Secure Signature Creation Device), tel qu'une carte à puce par exemple
- L'OID de Politique de Certification de l'AC émettrice du certificat est bien un des OID explicitement autorisés dans la politique de validation

3.2.5 Module W/R des fichiers de configuration

Ce module permet les opérations de traitement du fichier de configuration de DVS, et notamment les actions suivantes :

- Chargement
- Mise à jour
- Signature
- Vérification de l'intégrité

Le fichier de configuration contient en particulier la liste des utilisateurs et applications autorisés, l'association entre les transactions définies pour une application et les Politiques de Confiance DVS, ainsi que le paramétrage de ces Politiques de Confiance (dont font partie les politiques de signature utilisées pour les validations, ainsi que les politiques de signature des preuves).

3.2.6 Module d'appel OCSP

Ce module permet d'envoyer des requêtes de vérification de certificats en temps réel au serveur OCSP adéquat. Le traitement effectué par ce module est le suivant :

- Formatage de la requête OCSP (le module prépare la requête et y intègre un identifiant unique ou *nonce*)
- Connexion au serveur. Il peut s'agir d'un serveur accessible en HTTP ou HTTPS avec authentification du serveur et éventuellement du client.
- Envoi de la requête au serveur
- Réception de la réponse OCSP

- Vérification de l'identifiant (*nonce*) de la réponse (l'identifiant doit correspondre à celui envoyé lors de la requête)
- Vérification de la signature de la réponse OCSP (le certificat de signature du serveur OCSP est configuré dans DVS par un super-administrateur).

La réponse OCSP est ensuite insérée dans la preuve générée par DVS.

3.2.7 Module d'appel à un serveur d'horodatage

Le fonctionnement de ce module est similaire à celui du module d'appel OCSP.

Lors de la vérification du certificat de signature du jeton d'horodatage, le module s'assure que l'OID de la politique d'horodatage appliqué est bien un OID autorisé.

Une fois récupéré et vérifié, le jeton d'horodatage est inséré dans la preuve générée par DVS.

3.2.8 Module de synchronisation des CRL

Ce module prend en charge la mise à jour régulière des CRL depuis leurs points de publication. La fréquence de mise à jour de chaque CRL est configurable par un super-administrateur de la TOE.

Ce module gère le téléchargement par HTTP / HTTPS (sans authentification client) ainsi que par protocole LDAP / LDAPS.

3.2.9 Module d'écriture des pistes d'audit

Le moteur de génération des pistes d'audit crée un nouveau fichier à chaque modification de la configuration de DVS.

Dans le cas du HSM *nCipher*, ce fichier est marqué avec un numéro de séquence puis signé pour en garantir l'intégrité. La date et l'heure apposées sur les signatures des pistes d'audit proviennent de l'heure fournie par le système sur lequel tourne le DVS.

3.2.10 Moteur de génération de preuve

Lors du traitement d'une requête de vérification, en dernière étape, DVS constitue une preuve de vérification. Cette preuve est constituée de :

- Toutes les données envoyées par l'application lors de la requête de vérification
- Horodatage effectué à la réception de la requête
- Données de validation collectées par le moteur de validation de certificat : listes de révocation, certificats des Autorités de Certification, réponses OCSP
- Empreinte du fichier de configuration DVS utilisé
- Résultat de la validation

Cette preuve est formatée par ce composant au format XAdES.

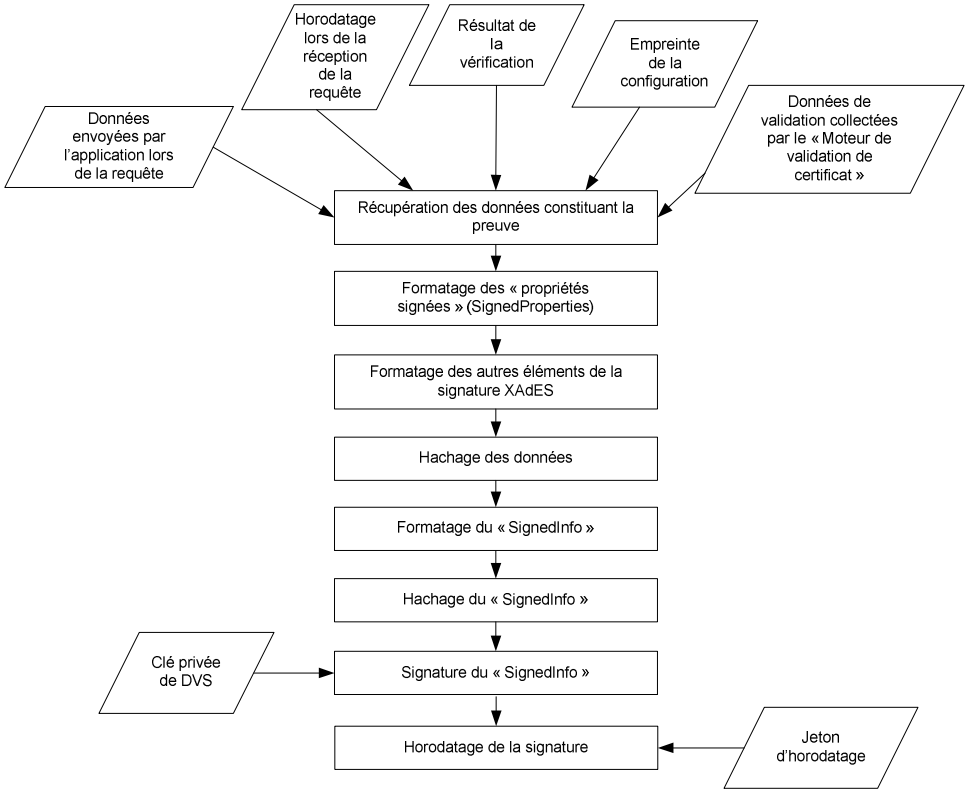


Figure 4 - Cinématique de génération et signature de la preuve de validation

3.2.11 Module de communication avec le dispositif de création de signature

Ce composant gère la communication avec le dispositif de signature externe, à savoir le boîtier cryptographique matériel (HSM) ou le module de signature exploitant les fichiers PKCS #12 contenus dans la base de données interne. Ce dispositif se charge de générer la signature au format PKCS #1 à partir du condensé qui lui est transmis.

Plusieurs modules font appel à lui :

- Le moteur de génération de preuve, qui demande à ce que la preuve formatée soit signée ;
- Le module W/R du fichier de configuration, qui demande à ce que le fichier de configuration soit signé ;
- Le module d'écriture de pistes d'audit, qui demande à ce que les fichiers d'audit soient signés ;
- Les modules d'appel vers des serveurs d'horodatage ou OCSP, qui peuvent se servir du HSM pour stocker la clé d'authentification-client SSL.

Dans la pratique, l'accès au dispositif de signature externe se fait au travers d'un *middleware* propre au dispositif de signature. Le composant de communication communique donc avec le *middleware*.

Les dispositifs de création de signature supportés par la TOE sont ceux présentant des interfaces conformes au standard PKCS #11. La TOE supporte ainsi nativement les boîtiers proposés par les principaux constructeurs :

- *nCipher* (retenu pour l'évaluation)
- *SafeNet*
- *Bull-Trustway*

3.2.12 Module de contrôle de sémantique

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

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

La TOE permet donc d'inclure, dans une politique de confiance, l'obligation de vérifier la stabilité sémantique d'un document dont on valide la signature. L'objectif de cette vérification est d'attester que la sémantique du document à signer « *ne dépend pas de paramètres qui lui sont extérieurs.* » **[EXT_DCSSI_PP, 2.4.2.1]**.

Néanmoins, le module de contrôle sémantique de DVS supporte moins de formats que le module de validation, ce qui peut amener à des situations dans lesquelles la politique requiert la vérification de la stabilité sémantique bien que DVS ne puisse pas l'effectuer. Dans ce cas, DVS signale l'absence de contrôle sémantique dans sa réponse et invalide la signature.

Pour résumer, le module opère comme suit :

1. Si le contenu du document est dans un format supporté par le module de validation, le contenu du document est examiné et le module répond « *stable* » ou « *unstable* » selon son diagnostic.
2. Dans tous les autres cas, le module répond que la sémantique du document n'a pas été vérifiée (« *not checked* » dans le profil de protection). La signature est invalidée par DVS.

Dans sa version actuelle, le module supporte le contrôle des formats « texte brut » (considéré comme « stable ») et « HTML » (l'Annexe A – Contrainte sur le format HTML, décrit le sous-ensemble du format considéré comme « stable » par le module).

3.3 Plateforme d'évaluation

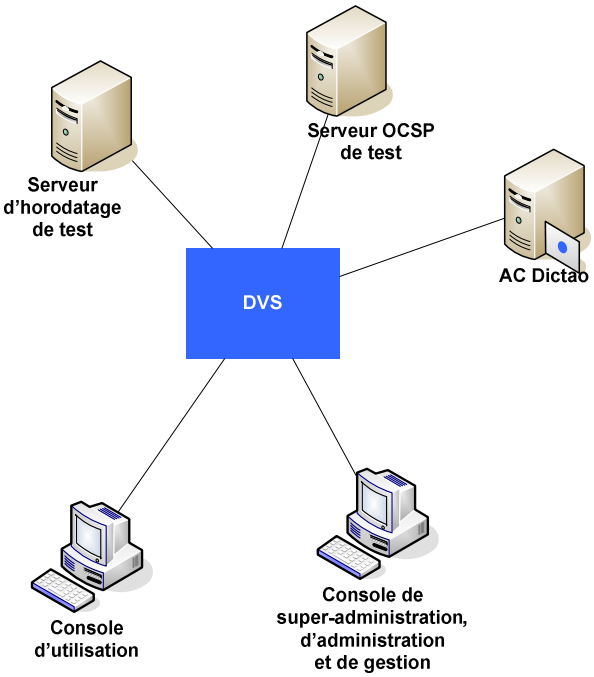
3.3.1 Plateforme Hôte

Le module de validation de signature DVS est évalué sur la configuration suivante :

- Ordinateur personnel
- Systèmes d'exploitation : **Sun Solaris 10**
- Base de données : **Oracle 10g**
- Serveur web : **Apache 2.2**
- Serveur d'applications : **Tomcat 5.0.28**
- Boîtier HSM : ***nCipher netShield*** (FIPS 140-2 Level-2)

3.3.2 Architecture de test

L'architecture suivante sera utilisée pour tester la TOE :



De plus, seront notamment utilisés durant les tests :

- Des fichiers signés (avec différents formats de signature) valides ou non
- Des certificats valides, non valides, révoqués, dont l'AC n'est pas connue de DVS, pour lequel le serveur OCSP n'est pas disponible, dont aucune CRL à jour n'est disponible, etc.
- Un serveur d'horodatage et un serveur OCSP accessibles ou non

3.3.3 Dispositif de création de signature

Le dispositif retenu pour l'évaluation est le *netShield* du constructeur *nCipher*. Ce boîtier est certifié FIPS 140-2 Level-2.

Il est utilisé pour stocker et utiliser les clés de signature suivantes : clé de signature du fichier de configuration, clé de signature des pistes d'audit, et clé de signature des preuves de validation.

3.3.4 Canaux de communication entre DVS, serveurs OCSP et IGC

Les protocoles de communication possibles entre les serveurs OCSP et les IGC et DVS sont HTTP, HTTPS, LDAP et LDAP+SSL.

L'administrateur, en configurant les adresses des OCSP et IGC, indique quel protocole utiliser.

Il est recommandé d'utiliser HTTPS ou LDAP+SSL.

Toutefois, ce protocole de communication n'influe pas sur la fiabilité des réponses des serveurs OCSP et des IGC car les fichiers envoyés sont signés et la signature vérifiée pas DVS. Si la signature n'est pas valide, le fichier n'est alors pas utilisé.

3.4 Visualisation du document

La TOE est un serveur de validation de signature et de certificats. Les exemples d'utilisation décrits au paragraphe 2.2.4 montrent que l'utilisateur[1] (vérificateur) est l'application appelante, donc un système automatisé.

La visualisation du document dans ce contexte concerne donc l'application appelante et les gestionnaires de la TOE, qui peuvent vouloir examiner les documents validés par celle-ci. Concernant l'application appelante, la TOE peut[2] renvoyer dans sa réponse le contenu du document dont la signature a été vérifiée. Ce contenu peut alors être affiché pour l'utilisateur final par l'application appelante ou au travers d'une application de visualisation externe.

Concernant la visualisation des documents validés par les gestionnaires de la TOE, les documents validés peuvent[2] être conservés dans les preuves archivées. Dans ce cas, la TOE propose aux gestionnaires la visualisation des documents contenus dans ces preuves par le biais du navigateur utilisé pour se connecter à la TOE ; ceci n'est possible que lorsqu'il s'agit de documents au format « texte » ou « HTML ». De plus, la liste des navigateurs dits « de référence » est définie par les administrateurs de la TOE dans la configuration de leurs politiques.

Pour les autres formats de documents, la TOE permet dans tous les cas de télécharger la preuve et donc d'accéder au document archivé, mais sans contrôle possible de l'interprétation qui sera faite de celui-ci.

[1] Le contexte est décrit au paragraphe 2.1 du document [EXT_DCSSI_PP].
[2] Suivant la configuration.

4. ENVIRONNEMENT DE SECURITE DE LA CIBLE D'EVALUATION

Ce paragraphe décrit l'environnement de sécurité de la cible d'évaluation :

- Les hypothèses d'utilisations
- Les menaces potentielles
- Les politiques de sécurité organisationnelles

4.1 Description des biens sensibles

Cette section décrit l'ensemble des biens sous le contrôle de la TOE.

4.1.1 Biens à protéger par la TOE

Ces données doivent être protégées en intégrité.

4.1.1.1 Données en entrée

B1. Document

Le document signé est le document signé par le signataire et pour lequel la TOE doit vérifier la signature (dans le cas de l'utilisation de la TOE pour une vérification de signature).

Ce document est fourni à la TOE dans le même fichier que la signature.

B2. Signature

La signature électronique d'un signataire sur le document (dans le cas de l'utilisation de la TOE pour une vérification de signature).

B3. Certificat

Le certificat à valider (dans le cas de l'utilisation de la TOE pour une validation seule de certificat).

B4. Attribut_ signés

Les attributs signés sont des données signées en même temps que le document. Elles fournissent à la TOE des précisions relatives à la signature et aux circonstances dans lesquelles elle a été effectuée.

Les attributs signés comprennent ~~entre autre~~ :

- La référence non ambiguë du certificat du signataire ou le certificat du signataire lui-même
- La politique de signature ou une référence à celle-ci
- Le type d'engagement du signataire
- Le rôle présumé ou certifié du signataire
- La date et l'heure présumée de signature
- Le lieu présumé de signature

Note : Les attributs signés sont fournis à la TOE dans le même fichier que la signature.

La politique de signature mentionnée ici est à distinguer des politiques de validation appliquées par la TOE : les politiques de (validation de) signature appliquées par la TOE à la

signature soumise par l'application cliente définissent les règles suivies par la TOE pour valider ou invalider une signature ; ces règles peuvent examiner, entre autres, la « politique de signature » incluse parmi ces attributs signés (0).

B5. Données_de_validation_en_entrée

Les données de validation sont les données utiles à la vérification, elles comprennent :

- Le certificat du signataire (est stocké dans la signature)
- Des certificats d'AC, d'émetteurs de CRL, de ~~réponses~~ serveur OCSP, de serveur d'horodatage (configurés par un super-administrateur de la TOE)
- Des listes de certificats révoqués (CRL) (téléchargés depuis des URL configurées par un super-administrateur de la TOE)
- Des réponses OCSP (renvoyées par des serveurs OSCP)
- Des listes d'autorités de certification révoquées (ARL)
- Des tampons d'horodatage (renvoyées par des serveurs OCSP)

4.1.1.2 Données de travail

B6. Données_à_vérifier_hachées

Les données à vérifier formatées sont les données sur lesquelles porte la signature (document et attributs signés), une fois hachées par la TOE.

En plus du statut de retour, la TOE renvoie à l'application cliente une preuve signée et horodatée par la TOE (le processus de création de preuve est décrit dans la Figure 4, p. 24). On distingue ici la preuve signée (bien B9) des données qu'elle contient (bien B7).

B7. Preuve

La preuve envoyée par la TOE contient les éléments suivants :

- Éléments envoyés par l'application
- Horodatage de réception de la signature
- Données de validation utilisées
- Empreinte de la configuration
- Statut de vérification

Ce bien représente la preuve (c.-à-d. tous ses éléments) avant signature.

4.1.1.3 Données en sortie

B8. Statut_de_retour

Après vérification, la TOE retourne un statut global de vérification qui dépend du résultat.

Dans le cas d'une vérification de signature :

- Signature valide : tous les éléments nécessaires sont présents et corrects.
- Signature invalide : un ou plusieurs sont incorrects.
- ~~Validation incomplète : des données n'étaient pas disponibles au moment de la vérification.~~

Dans le cas d'une validation de certificat :

- Certificat valide
- Certificat invalide

À ce statut global est associé un statut détaillé du résultat des différentes étapes de validation.

B9. Preuve_signée

Ce bien est la preuve (B7) signée au format XAdES.

B10. Données_de_validation_en_sortie

Les données de validation en sortie sont les données de validation traitées par la TOE.

Elles sont retournées par la TOE ~~au vérificateur~~ à l'application cliente pour usage ultérieur.

~~Ces données peuvent être complètes ou non. Si elles le sont, alors elles pourront servir à une vérification ultérieure. Sinon, elles pourront être réutilisées et enrichies dans le cadre d'une nouvelle vérification immédiate.~~

Note : Ces données sont complètes et font partie de la preuve signée (B9.Preuve_signée).

B11. Pistes_d'audit

Les pistes d'audit sont des fichiers générés par la TOE après chaque session d'un administrateur ou d'un super-administrateur. Ces fichiers contiennent la liste des actions effectuées par celui-ci au cours d'une session et doivent être protégés en intégrité.

4.1.2 Biens sensibles de la TOE

B12. Service

Ce bien représente le code exécutable implémentant les services rendus.

Le code de la TOE doit être protégé en intégrité.

B13. Règles_de_vérification

Le cœur de la TOE est constitué d'un moteur vérifiant des règles sur la base d'une politique de signature.

Le code exécutable implémentant ces règles dans l'application requiert une protection en intégrité.

La politique de signature mentionnée ici est la politique de validation appliquée par la TOE.

B14. Configuration_du_service

La configuration du service définit tous les paramètres de configuration de la TOE

- Liste des super-administrateurs autorisés
- Liste des administrateurs autorisés
- Liste des gestionnaires autorisés
- Liste des super-gestionnaires autorisés
- Liste des applications clientes autorisées et des transactions possibles pour chaque application
- Liste et paramétrage des politiques de signature
- Correspondance entre transaction d'une application et politique de confiance

La configuration du service doit être protégée en intégrité.

Les politiques de signature mentionnées ici sont les politiques de validation appliquées par la TOE, en tant que partie des politiques de confiance (3.1.2).

B15. Politique_de_signature

Les politiques de signature définissent les règles à appliquer pour vérifier une signature donnée.

La TOE supporte ~~une ou~~ plusieurs politiques de signature. La liste des politiques de signature, qui est gérée par l'administrateur de la TOE, doit être protégée en intégrité. De plus, l'intégrité de chacune des politiques de signature doit aussi être contrôlée.

Cette donnée fait partie des données de configuration du service (B14.Configuration_du_service).

Les politiques de signature mentionnées ici sont les politiques de validation appliquées par la TOE, en tant que partie des politiques de confiance (3.1.2).

B16. Correspondance_données_internes/externe

Les données internes du module possèdent souvent une représentation différente de celles présentées à l'utilisateur ou entrées dans le module.

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

B17. B.Correspondance_FormatDoc_Application

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

L'intégrité de ce bien doit être protégée.

Note d'application : Le format du document est

- soit fourni par le vérificateur,
- soit présent dans la signature en tant qu'attribut signé.

Note d'application : ce bien représente les applications de référence sélectionnées par les administrateurs dans leurs politiques.

4.1.3 Sujets

~~S.Vérificateur~~

~~La TOE peut être invoquée par un être humain ou une application appelante. Le vérificateur désigne l'entité invoquant les fonctions de la TOE pour vérifier une signature.~~

S1. Application_cliente

L'application cliente est l'application effectuant une requête de vérification à DVS : elle invoque les fonctions de la TOE pour vérifier une signature ou un certificat

Note : Ce sujet est identique à celui défini par S.Vérificateur dans le profil de protection

S2. Super-Administrateur_de_sécurité

Les super-administrateurs de sécurité (ou « super-administrateurs ») de la TOE sont en charge des opérations suivantes :

- Gérer les administrateurs, les super-administrateurs, les super-gestionnaires du service
- Gérer les ressources accessibles aux administrateurs de sécurité (serveur d'horodatage, OCSP, autorité de certification référencées…)
- Vérifier les pistes d'audit de la TOE

S3. Administrateur_de_sécurité

Les administrateurs de sécurité (ou « administrateurs ») de la TOE sont en charge des opérations suivantes :

- ~~dans le cas où la TOE utilise des politiques de signature paramétrables, il~~ La TOE utilisant des politiques de signatures paramétrables, l'administrateur de sécurité maintient les politiques de signature utilisables (ajout, suppression)
- gère la correspondance entre les formats de document présentés et les applications permettant leur présentation au vérificateur
- ~~gère la liste des formats de document garantissant la stabilité de sémantique du document dans le temps.~~
- Gérer les applications de leur groupe autorisées à effectuer des requêtes
- Gérer les administrateurs et gestionnaires de leur groupe
- Gérer la table d'association spécifiant à quelles politiques de confiance peuvent accéder quelles applications clientes.
- Vérifier les données d'audit de son groupe

S4.	Gestionnaire_de_la_TOE

Les gestionnaires de la TOE accèdent aux données de gestion de leur groupe, à savoir :

- Récapitulatifs des transactions du groupe effectuées par mois
- Recherche multicritère dans les transactions archivées du groupe
- Rapports de service du groupe (nombre de transactions par application, transaction…)

Note :

Les rôles d'administrateur de sécurité de la TOE et de super-administrateur de sécurité de la TOE sont distincts du rôle d'administrateur (appelé ici « opérateur ») de la machine sur laquelle la TOE s'exécute.

S5.	Super-Gestionnaire_de_la_TOE

Les super-gestionnaires de la TOE accèdent aux données de gestion de la TOE, à savoir :

- Récapitulatifs des transactions effectuées par mois
- Recherche multicritère dans les transactions archivées
- Rapports de service (nombre de transactions par application, transaction…)

Note : contrairement aux gestionnaires, qui ne peuvent consulter que les données de gestion du groupe qu'ils gèrent, les super-gestionnaires peuvent consulter les données de tous les groupes.

4.2 Hypothèses

H1.	Machine_Hôte

On suppose que la machine hôte sur laquelle la TOE s'exécute est ~~soit directement sous la responsabilité du vérificateur soit~~ sous la responsabilité d'une personne morale ou physique qui lui garantit que les mesures ci-après sont bien appliquées.

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~~ opérateurs 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~~ l'opérateur
- 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 (l'opérateur) mentionné ci-dessus est distinct de celui d'administrateur de sécurité de la TOE.
- Cette hypothèse couvre des menaces où des processus informatiques viendraient perturber l'exécution des services de la TOE et par exemple modifier les données utilisateur telles que les certificats et données de validation lorsqu'elles sont sous son contrôle.

H2. Poste_(Super-)Administrateur

On suppose que la machine à partir de laquelle les administrateurs ou les super-administrateurs accèdent aux fonctions d'administration est sous la responsabilité d'une personne morale ou physique qui lui garantit que les mesures ci-après sont bien appliquées.

Le système d'exploitation de la machine 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 est protégée contre les virus
- Les échanges entre la machine 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 est restreint aux seuls opérateurs de celle-ci (différenciation compte utilisateur/administrateur)
- L'installation et la mise à jour de logiciels sur la machine sont sous le contrôle de l'opérateur de la machine
- Le système d'exploitation de la machine refuse l'exécution d'applications téléchargées ne provenant pas de sources sûres

Note d'application :

- Le rôle d'opérateur mentionné ci-dessus est distinct de celui d'administrateur de sécurité de la TOE.

H3. Poste_Gestionnaire

On suppose que la machine à partir de laquelle les gestionnaires et les super-gestionnaires accèdent aux fonctions de gestion est sous la responsabilité d'une personne morale ou physique qui lui garantit que les mesures ci-après sont bien appliquées.

Le système d'exploitation de la machine 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 est protégée contre les virus
- Les échanges entre la machine 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 est restreint aux seuls opérateurs de celle-ci (différenciation compte utilisateur/administrateur)
- L'installation et la mise à jour de logiciels sur la machine est sous le contrôle de l'opérateur de la machine
- Le système d'exploitation de la machine refuse l'exécution d'applications téléchargées ne provenant pas de sources sûres

Note d'application :

- Le rôle d'opérateur mentionné ci-dessus est distinct de celui d'administrateur de sécurité de la TOE.

H4. (Super-)Administrateur_De_Sécurité_Sûr

Les administrateurs et les super-administrateurs de sécurité de la TOE sont supposés être de confiance, formé à l'utilisation de la TOE et disposant des moyens nécessaires à la réalisation de leur activité.

Les administrateurs et les super-administrateurs de sécurité de la TOE configurent correctement les politiques de signature de la TOE et s'assurent, le cas échéant, de la validité des OID utilisées pour les référencer.

H5. Gestionnaire_Sûr

Les gestionnaires et super-gestionnaires de la TOE sont supposés être de confiance, formés à l'utilisation de la TOE et disposant des moyens nécessaires à la réalisation de leur activité.

H6. Application_Cliente_Sûre

L'application cliente est supposée être de confiance, développée en conformité aux recommandations se trouvant dans le guide de développement d'applications appelantes.

H7. Politique_Signature_D'Origine_Authentique

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

Note d'application

- Cette hypothèse se justifie ainsi:

  Pour vérifier l'authenticité de l'origine d'une politique de signature, il faudrait par exemple vérifier la signature que son émetteur y aurait associée. Pour ce faire, il faudrait alors utiliser une autre politique de signature dont l'authenticité de l'origine resterait à prouver... ce processus serait sans fin.
- Cette hypothèse est remplie *de facto* si la TOE n'utilise pas de politiques de signature interprétées mais des politiques fixes.

Les politiques de signature mentionnées ici sont les politiques de validation appliquées par la TOE, en tant que partie des politiques de confiance (3.1.2). Ces politiques sont transcrites par les administrateurs (définition des transactions) et super-administrateurs (spécification des règles et des ressources disponibles) dans les fichiers de configuration de la TOE.

H8. Présentation_Document

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

- Soit retranscrivent fidèlement le document à vérifier,
- Soit préviennent le ~~vérificateur~~ l'utilisateur final des éventuels problèmes d'incompatibilité du dispositif de présentation avec les caractéristiques du document.

Dans le cas d'une contre-signature, on suppose que l'application de présentation indique au moins l'identité du ou des signataires précédents, et au mieux vérifie cette ou ces signatures.

Note d'application :

Pour les applications clientes, la TOE n'invoque pas elle-même l'application de visualisation du document signé. Elle transmet le contenu du document dont la signature a été vérifiée (ce contenu est présent dans la réponse de la validation de signature). L'application appelante (qui est en fait le vérificateur au regard du système dans lequel s'intègre la TOE) peut ensuite afficher à l'utilisateur humain –s'il est présent et s'il doit en avoir connaissance (cas de la gestion d'identité §2.2.4)– ce contenu.

Par ailleurs, si la configuration le permet, la TOE propose aux gestionnaires la visualisation des documents (formats texte et HTML vérifiés sémantiquement) contenus dans les preuves archivées par le biais du navigateur utilisé par ceux-ci pour se connecter à la TOE.

L'activation de la visualisation est contrôlée au niveau des politiques de confiance par les administrateurs de la TOE.

~~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 d'application :

Le contrôle d'invariance est réalisé par la TOE.

H9. Intégrité_Services

On suppose que l'environnement de la TOE fournit à l'administrateur de sécurité les moyens de contrôler l'intégrité des services de la TOE.

H10. Accès_Données_De_Validation

La TOE doit disposer de – ou avoir accès à – toutes les données de validation nécessaires à la vérification de la signature d'un document selon la politique de signature à appliquer.

H11. Analyse_Périodique_journaux

Les administrateurs et super-administrateurs de DVS analysent périodiquement les pistes d'audit afin de s'assurer du bon fonctionnement de la TOE.

H12. Suppression_Périodique_journaux

La TOE ne permettant pas la suppression des pistes d'audit, les *opérateurs de la machine* les effacent régulièrement afin de s'assurer qu'elles ne satureront pas le ou les disques de stockage.

Note :

Il s'agit-là des pistes d'audit générées par DVS. Ces pistes d'audit ne sont pas effaçables à travers l'interface d'administration de DVS. Seul l'opérateur d'hébergement de la machine sur laquelle se trouve DVS peut les effacer.

H13. Protection_Moyens_Authentification

On suppose que les mots de passe ou autres moyens d'authentification des utilisateurs (administrateurs, super-administrateurs, gestionnaires et super-gestionnaires) sont protégés par les utilisateurs de manière à maintenir les objectifs de sécurité de la TOE.

H14. Protection_HSM

On suppose que l'activation et l'administration du boîtier cryptographique (utilisé par la TOE) sont protégées à un niveau adéquat. Pour cela l'utilisation de cartes à puces selon une stratégie n sur m, n étant supérieur ou égal à 2 (nombre minimum de cartes nécessaire à l'utilisation des fonctions d'administration) est recommandée. On suppose aussi que les codes PIN associés à ces cartes sont suffisamment complexes.

H15. Authentification_Mutuelle

Un module externe à la TSF permet d'effectuer une authentification mutuelle entre la TOE et les utilisateurs (S1.Application_cliente, S2.Super-Administrateur_de_sécurité, S3.Administrateur_de_sécurité, S4.Gestionnaire_de_la_TOE, S5.Super-Gestionnaire_de_la_TOE) afin de se protéger contre l'usurpation d'identité.

Notes :

En plus de cette authentification externe, la TOE contrôle par elle-même la validité du certificat présenté et s'il est autorisé à accéder au service qu'il demande. La TOE constitue ensuite une preuve de ce contrôle.

De plus, lors d'une modification de la configuration, l'administrateur ou le super-administrateur signe le nouveau fichier de configuration. La TOE vérifie alors elle-même la signature du fichier

de configuration avant de prendre en compte la modification.

H16. Protection_Clé_Signature_Configuration

On suppose que la clé privée utilisée pour la signature du fichier de configuration est protégée de manière adéquate, par exemple au travers d'un HSM (protection supérieure à celle des clés privées utilisées lors de l'authentification mutuelle).

H17. Protection_Communications

Les communications entre la TOE et les machines des utilisateurs (S1.Application_cliente, S2.Super-Administrateur_de_sécurité, S3.Administrateur_de_sécurité, S4.Gestionnaire_de_la_TOE, S5.Super-Gestionnaire_de_la_TOE) sont protégées en confidentialité et intégrité par un module externe à la TSF. La protection est implémentée conformément aux recommandations de la DCSSI [CRYPT_STD].

H18. Services_Tiers_De_Confiance

On suppose que les OCSP, IGC et serveurs d'horodatage auxquels la TOE fait une requête fournissent des informations fiables.

4.3 Menaces

M1. Modification_Ens_Politiques_Signature

Un utilisateur malveillant peut ajouter ou supprimer de manière illicite des politiques de signature à l'ensemble des politiques de signature supportées par la TOE.

Selon l'opération effectuée, ceci peut aboutir :

- Dans le cas d'un ajout de politiques, à une validation de signatures non vérifiables sinon.
- Dans le cas d'une suppression de politiques, à une impossibilité de vérifier des signatures jusqu'alors acceptées.

De plus, un utilisateur malveillant peut ajouter ou supprimer de manière illicite :

- des utilisateurs (super-administrateur, administrateur, gestionnaire ou super-gestionnaire)
- des applications autorisées à se connecter
- des associations politique de confiance / application

Les politiques de signature mentionnées ici sont les politiques de validation appliquées par la TOE, en tant que partie des politiques de confiance (3.1.2).

4.4 Politiques de sécurité organisationnelles

4.4.1 Politiques relatives à l'application d'une politique de signature

Les politiques de signature mentionnées dans cette partie sont les politiques de validation appliquées par la TOE, en tant que partie des politiques de confiance (3.1.2).

P1. Validité_Certificat_Signataire

La TOE doit contrôler que le certificat du signataire est bien en cours de validité.

P2. Conformité_Attributs_Signés

La TOE doit contrôler :

- Que les attributs signés sont bien conformes à la politique de signature à appliquer
- Que tous les attributs de signature requis par la politique de signature sont présents.

P3. Conformité_Certificat_Signataire

La TOE doit contrôler que tous les certificats du chemin de certification (comprenant le certificat du signataire) sont bien conformes à la politique de signature appliquée.

P4. Authenticité_Certificat_Signataire

La TOE doit contrôler qu'un chemin de certification valide(1) existe entre le certificat du signataire et un point de confiance référencé dans la politique de signature.

(1) L'existence d'un tel chemin de validation prouve l'authenticité du certificat du signataire par rapport au certificat racine (point de confiance).

P5. Authenticité/Intégrité_Données_Validation

La TOE doit contrôler l'authenticité de l'origine et l'intégrité des données de validation fournies.

4.4.2 Communication des attributs signés

P6. Communication_Attributs_Signés

La TOE doit permettre de communiquer les attributs signés ~~au vérificateur~~ à l'application cliente.

4.4.3 Présentation du document au vérificateur

P7. Possibilité_Présenter_Document

La TOE pourra permettre au vérificateur de visualiser le document signé (Décret 2001-272, Art 5 alinéa c).

Cette capacité sera désactivable par un administrateur de la TOE, pour le cas où le vérificateur est une machine (voir politique P.Administration).

Les administrateurs de la TOE doivent définir, dans le cadre de leurs politiques de validation, des applications de référence pour la visualisation du document signé, en fonction des formats supportés par la politique.

Note d'application

Les fonctionnalités de la TOE s'adressant en premier lieu à une application appelante, la présentation n'est pas effectuée par la TOE elle-même, toutefois, cette dernière transmet (O17.Export_Contenu) le contenu du document dont la signature a été vérifiée à l'application appelante afin que cette dernière puisse connaître exactement les données qui ont été signées.

Par ailleurs, si la configuration le permet, la TOE propose aux gestionnaires et super-gestionnaires la visualisation des documents (formats texte et HTML vérifiés sémantiquement) contenus dans les preuves archivées par le biais du navigateur utilisé par ceux-ci pour se connecter à la TOE.

L'activation de la visualisation est contrôlée au niveau des politiques de confiance par les administrateurs de la TOE.

P8. Sémantique_Document_Invariante

La TOE doit prévenir le vérificateur si la sémantique du document signé est instable ou peut être instable.

Note :

La TOE effectue elle-même le contrôle de sémantique.

4.4.4 Conformité aux standards

P9. Algorithmes_De_Hachage

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

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

P10. Algorithmes_De_Signature

Les algorithmes cryptographiques supportés et les longueurs des clés mises en œuvre par la TOE devront résister durant la durée de validité des certificats de clé publique de ces clés.

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

Note : Tous les algorithmes cryptographiques utilisés dans le processus de vérification de la signature électronique doivent résister aux attaques par cryptanalyse. En particulier la taille des clefs devra être suffisamment grande pour assurer la résistance de la clef publique présente dans un certificat pendant la durée de validité de ce dernier.

4.4.5 Export des données de validation

P11. Export_Contenu

La TOE doit transmettre dans sa réponse le contenu du document dont la signature a été vérifiée ou celui du certificat qui a été validé.

P12. Export_Données_Validation

La TOE doit permettre d'exporter ~~au vérificateur~~ à l'application appelante les données de validation utilisées lors de la vérification de la signature ou la validation du certificat.

P13. Export_Résultat_Validation

La TOE doit exporter à l'application appelante le résultat de vérification de signature ou de la validation de certificat.

4.4.6 Divers

P14. Super-Administration

La TOE doit permettre au super-administrateur de sécurité de :

- Gérer les administrateurs, super-administrateurs et super-gestionnaires du service
- Gérer les ressources accessibles aux administrateurs de sécurité (serveur d'horodatage, OCSP, autorité de certification référencées…)
- Vérifier les données d'audit

P15. Administration

La TOE doit permettre à l'administrateur de sécurité de ~~gérer~~ :

- Gérer les politiques de signatures paramétrables [B15.Politique_de_signature] (ajout, suppression)
- Gérer les applications de leur groupe autorisées à effectuer des requêtes
- Gérer les administrateurs et gestionnaires de leur groupe
- Gérer l'association entre politiques de confiance et applications clientes par le biais de transactions.
- Vérifier les données d'audit de son groupe
- la table de correspondance entre les applications de visualisation et les formats de documents en entrée de la TOE [B.Correspondance_FormatDoc_Application].
- ainsi que d'inhiber la fonction de visualisation du document signé.

Note d'application :

L'association entre politiques de confiance et applications clientes passe par l'intermédiaire des transactions : à toute transaction est associée une politique de confiance, et une application n'a accès qu'à un certain nombre de transactions, définies par l'administrateur de sécurité.

La correspondance entre les applications de visualisation et les formats de documents (B.Correspondance_FormatDoc_Application) est gérée par les administrateurs dans la définition des politiques de confiance (voir note d'application de la politique P7.Possibilité_Présenter_Document, p. 38).

P16. Gestion

La TOE doit permettre au gestionnaire d'accéder aux données de gestion de la TOE:

- Transactions effectuées
- Rapport de service

Note : le terme « transaction effectuée » désigne les différentes requêtes soumises par les applications clientes (validation de signature, de certificat).

P17. Audit

La TOE doit enregistrer les actions effectuées par un super-administrateur de la TOE et ne permettre la présentation de ces traces (pistes d'audit) qu'aux seuls super-administrateurs de la TOE.

La TOE doit enregistrer les actions effectuées par un administrateur de la TOE et ne permettre la présentation de ces traces (pistes d'audit) qu'aux seuls administrateurs et super-administrateurs de la TOE.

La TOE ne doit pas permettre aux utilisateurs de la TOE (sujets S1.Application_cliente, S2.Super-Administrateur_de_sécurité, S3.Administrateur_de_sécurité, S4.Gestionnaire_de_la_TOE, S5.Super-Gestionnaire_de_la_TOE) d'effacer les pistes d'audit, et toute modification sur celles-ci doit être détectée.

Note :

L'effacement des pistes d'audit n'est possible que par l'opérateur d'hébergement au travers de l'interface du système d'exploitation de la machine (H12)

5. OBJECTIFS DE SECURITE

5.1 Objectifs de sécurité sur la TOE

5.1.1 Objectifs généraux

O1. Authentification_Utilisateurs

Les utilisateurs de la TOE devront s'authentifier avant de pouvoir accéder aux fonctions/services de la TOE.

O2. Super-administration

La TOE devra permettre à un super-administrateur de sécurité de :

- Gérer les administrateurs, super-administrateurs, gestionnaires et super-gestionnaires du service
- Gérer les ressources accessibles aux administrateurs de sécurité (serveurs d'horodatage, OCSP, autorités de certification référencées…)

O3. Administration

La TOE devra permettre à l'administrateur de sécurité de :

- Gérer les politiques de signature (ajout, suppression)
- gère la correspondance entre les formats de document présentés et les applications permettant leur présentation au vérificateur
- Gérer les applications de leur groupe autorisées à effectuer des requêtes
- Gérer les administrateurs et gestionnaires de leur groupe
- Gérer la table d'association spécifiant à quelles politiques de confiance peuvent accéder quelles applications clientes.
- la table de correspondance entre les applications de visualisation et les formats de documents en entrée de la TOE.
- ainsi que d'inhiber la fonction de visualisation du document signé.

Note d'application : La correspondance entre les applications de visualisation et les formats de documents (B.Correspondance_FormatDoc_Application) est gérée par les administrateurs dans la définition des politiques de confiance (voir note d'application de la politique P7.Possibilité_Présenter_Document, p. 38).

O4. Gestion

La TOE devra permettre au gestionnaire d'accéder aux données de gestion de la TOE:

- Transactions effectuées
- Rapport de service

Note : le terme « transaction effectuée » désigne les différentes requêtes soumises par les applications clientes (validation de signature, de certificat).

O5. Audit

La TOE doit enregistrer les actions effectuées par un super-administrateur de la TOE et ne permettre la présentation de ces traces (pistes d'audit) qu'aux seuls super-administrateurs de la TOE.

La TOE doit enregistrer les actions effectuées par un administrateur de la TOE et ne permettre la présentation de ces traces (pistes d'audit) qu'aux seuls administrateurs de la TOE.

La TOE ne doit pas permettre aux utilisateurs de la TOE (sujets S1.Application_cliente, S2.Super-Administrateur_de_sécurité, S3.Administrateur_de_sécurité, S4.Gestionnaire_de_la_TOE, S5.Super-Gestionnaire_de_la_TOE) d'effacer les pistes d'audit, et toute modification sur celles-ci doit être détectée.

5.1.2 Objectifs sur la configuration de la TOE

O6. Gestion_Politiques_De_Signature

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

O7. Gestion_Configuration

La TOE ne devra permettre la modification de l'ensemble de la configuration qu'aux administrateurs et aux super-administrateurs de la TOE.

5.1.3 Objectifs sur les rapports de transactions

O8. Revue_Rapports

La TOE devra identifier les opérateurs avant d'autoriser la lecture de l'ensemble des données sur les transactions et requêtes effectuées auprès de DVS.

5.1.4 Objectifs sur les règles de vérification

Les politiques de signature mentionnées ici sont les politiques de validation appliquées par la TOE, en tant que partie des politiques de confiance (3.1.2).

O9. Référence_De_Temps

Conformément à la politique de signature appliquée, la TOE devra s'assurer de la présence d'une référence de temps de confiance qui permette d'attester de l'existence de la signature numérique à une date donnée.

Note d'application

Par référence de temps de confiance on comprend ici tout moyen permettant d'obtenir une référence de temps de manière sûre pour le contexte d'utilisation de la TOE. Ce moyen est défini par la politique de signature.

Une référence de temps de confiance peut par exemple être :

- Un tampon d'horodatage signé par une entité de confiance, conformément à la politique de signature
- Une marque de temps fournie par un acteur de confiance, conformément à la politique de signature

O10. Chemin_De_Certification

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

- Le certificat du signataire dont la référence est fournie dans les attributs signés, et

- Un point de confiance référencé dans la politique de signature.

O11. Conformité_Des_Certificats

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

O12. Validité_Des_Certificats

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

- l'intégrité et l'authenticité de l'origine du certificat;
- que le certificat était en cours de validité au moment où la signature numérique a été positionnée dans le temps;
- que le certificat n'était pas révoqué au moment où la signature numérique a été positionnée dans le temps.

O13. Conformité_Données_Validation

La TOE doit vérifier que les données de validation fournies pour vérifier la signature répondent bien aux critères de la politique de signature appliquée, notamment qu'elles sont signées par leur émetteur (intégrité et authenticité de l'origine).

Note d'application

La signature des données de validation fournies permet de garantir à la fois l'intégrité de ces données et l'authenticité de leur origine, conformément à la politique de signature appliquée.

O14. Conformité_Attributs_Signés

La TOE doit vérifier la présence et la conformité des attributs signés en regard de la politique de signature.

5.1.5 Objectifs relatifs à la visualisation des données signées

O15. Lancement_Applications_Présentation

La TOE devra pouvoir lancer des applications externes pour permettre au vérificateur de visualiser le document dont la signature est à vérifier. Pour cela elle se basera sur l'indication du format du document fournie dans la signature électronique à vérifier.

Un paramètre de configuration permettra à un super-administrateur de la TOE de désactiver cette fonction au moment de l'installation de la TOE si l'utilisateur est une machine.

Note d'application

Les fonctionnalités de la TOE s'adressant en premier lieu à une application appelante, la présentation n'est pas effectuée par la TOE elle-même, toutefois, cette dernière transmet (O17.Export_Contenu) le contenu du document dont la signature a été vérifiée à l'application appelante afin que cette dernière puisse connaître exactement les données qui ont été signées.

Par ailleurs, si la configuration le permet, la TOE propose aux gestionnaires la visualisation des documents (formats texte et HTML vérifiés sémantiquement) contenus dans les preuves archivées par le biais du navigateur utilisé par ceux-ci pour se connecter à la TOE.

L'activation de la visualisation est contrôlée au niveau des politiques de confiance par les administrateurs de la TOE. Au moment de l'installation de la TOE, c'est le super-administrateur qui installe la toute première politique de confiance et définit donc si la visualisation est activée

ou non.

O16. Communication_Attributs_Signés

La TOE devra permettre de communiquer les attributs signés ~~au vérificateur~~ à l'application appelante.

Note d'application

Cet objectif s'applique de manière identique aux cas où l'utilisateur est un humain et à celui où c'est une machine et quels que soient les moyens utilisés pour les communiquer: une interface homme-machine ou une interface programmatique (API).

O17. Export_Contenu

La TOE devra transmettre dans sa réponse le contenu du document dont la signature a été vérifiée ou celui du certificat qui a été validé.

O18. Export_Données_Validation

La TOE devra permettre d'exporter ~~au vérificateur~~ à l'application appelante les données de validation utilisées lors de la vérification de la signature ou la validation du certificat.

Les politiques de signature mentionnées ici sont les politiques de validation appliquées par la TOE, en tant que partie des politiques de confiance (3.1.2).

O19. Export_Résultat_Validation

La TOE devra exporter à l'application appelante le résultat de validation de signature ou de la validation de certificat.

5.1.6 Objectifs relatifs au contrôle d'invariance de la sémantique du document à vérifier

O20. Invocation_Module_Controle_Invariance

~~Pour chaque document,~~ La TOE devra interroger un module ~~externe~~ interne chargé d'identifier si la sémantique du document est bien invariante.

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

5.1.7 Conformité aux standards

O21. Support_Cryptographique

La TOE devra supporter des algorithmes cryptographiques ayant les propriétés suivantes :

- les algorithmes de hachage ne permettent pas de créer deux documents produisant le même condensé.
- les algorithmes cryptographiques supportés et les longueurs des clés mises en œuvre par la TOE devront résister durant la durée de validité des certificats de clé publique de ces clés.

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

5.1.8 Protection des données

O22. Protection_données_de_configuration

Les modifications non autorisées des données de configuration doivent être détectées.

O23. Protection_pistes_audit

Les modifications non autorisées des pistes d'audit de DVS doivent être détectées.

5.2 Objectifs de sécurité sur l'environnement de la TOE

OE1. Authenticité_Origine_Politique_Signature

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

OE2. Machine_Hôte

La machine hôte sur laquelle la TOE s'exécute devra être ~~soit directement sous la responsabilité du vérificateur soit~~ sous la responsabilité d'une personne morale ou physique qui lui garantit que les mesures ci-après sont bien appliquées.

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

De plus 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 opérateurs 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'opérateur;
- 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'opérateur de la machine hôte mentionné ci-dessus est distinct de celui d'administrateur de sécurité de la TOE.

OE3. Poste_(Super-)Administrateur

La machine à partir de laquelle les administrateurs et les super-administrateurs accèdent aux fonctions d'administration devra être sous la responsabilité d'une personne morale ou physique qui lui garantit que les mesures ci-après sont bien appliquées.

Le système d'exploitation de la machine 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 est protégée contre les virus
- Les échanges entre la machine 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 est restreint aux seuls opérateurs de celle-ci (différenciation compte utilisateur/administrateur)
- L'installation et la mise à jour de logiciels sur la machine est sous le contrôle de l'opérateur de la machine
- Le système d'exploitation de la machine refuse l'exécution d'applications téléchargées ne provenant pas de sources sûres

Note d'application :

- Le rôle d'opérateur de la machine mentionné ci-dessus est distinct de celui d'administrateur de sécurité de la TOE.

OE4. Poste_Gestionnaire

La machine à partir de laquelle les gestionnaires ou les super-gestionnaires accèdent aux fonctions de gestion devra être sous la responsabilité d'une personne morale ou physique qui lui garantit que les mesures ci-après sont bien appliquées.

Le système d'exploitation de la machine 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 est protégée contre les virus
- Les échanges entre la machine 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 est restreint aux seuls opérateurs de celle-ci (différenciation compte utilisateur/administrateur)
- L'installation et la mise à jour de logiciels sur la machine est sous le contrôle de l'opérateur de la machine
- Le système d'exploitation de la machine refuse l'exécution d'applications téléchargées ne provenant pas de sources sûres

Note d'application :

- Le rôle d'opérateur de la machine mentionné ci-dessus est distinct de celui d'administrateur de sécurité de la TOE.

OE5. Présentation_Document

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

- Soit retranscrivent fidèlement le document à vérifier
- Soit préviennent le ~~vérificateur~~ l'utilisateur final des éventuels problèmes d'incompatibilité du dispositif de présentation avec les caractéristiques du document

Les politiques de validation de la TOE doivent définir, en fonction des formats supportés par celle-ci, des applications de référence pour la visualisation du document signé.

Note d'application :

Se référer à la note de l'hypothèse H8.Présentation_Document.

~~OE.Contrôle_Sémantique_Document_Signé~~

~~L'environnement de la TOE devra fournir un module capable de déterminer si la sémantique du document signé :~~

- ~~Soit est bien invariante~~
- ~~Soit est instable~~
- ~~Soit n'a pas pu être vérifiée (par exemple faute de pouvoir supporter ce format).~~

~~Ce module doit communiquer le statut de son analyse à la TOE.~~

Note d'application :

Se référer à la note de l'hypothèse H.Contrôle_Invariance_Sémantique_Document.

OE6. (Super-)Administrateur_De_Sécurité_Sûr

Les administrateurs et les super-administrateurs de sécurité de la TOE ~~est~~ sont de confiance, formés à l'utilisation de la TOE et disposent des moyens nécessaires à la réalisation de leur activité.

Les administrateurs et les super-administrateurs de sécurité de la TOE doivent configurer correctement les politiques de signature de la TOE et s'assurer, le cas échéant, de la validité des OID utilisées pour les référencer.

OE7. Gestionnaire_Sûr

Les gestionnaires et super-gestionnaires de la TOE sont de confiance, formés à l'utilisation de la TOE et disposent des moyens nécessaires à la réalisation de leur activité.

OE8. Application_Cliente_Sûre

L'application appelante est de confiance, développée en conformité aux recommandations se trouvant dans le guide de développement d'applications appelantes.

OE9. Fourniture_Des_Données_De_Validation

L'environnement de la TOE devra lui fournir les données de validation nécessaires à la vérification de la signature.

OE10. Intégrité_Services

L'environnement de la TOE devra fournir aux administrateurs de sécurité les moyens de contrôler l'intégrité des services de la TOE.

OE11. Analyse_Périodique_Journaux

Les *super-administrateurs de sécurité* doivent analyser périodiquement les pistes d'audit afin de s'assurer du bon fonctionnement de la TOE.

OE12. Suppression_Périodique_journaux

Les *opérateurs d'hébergement* doivent sauvegarder régulièrement les pistes d'audit afin de prévenir toute saturation des disques de stockage.

OE13. Protection_Moyens_Authentification

Les mots de passe ou autres moyens d'authentification des utilisateurs (*(super-) administrateurs* et *gestionnaires)* doivent être protégés par les utilisateurs de manière à maintenir les objectifs de sécurité de la TOE.

OE14. Protection_HSM

L'activation et l'administration du boîtier cryptographique (utilisé par la TOE) doivent être protégées à un niveau adéquat. Pour cela l'utilisation de cartes à puces selon une stratégie n sur m, n étant supérieur ou égal à 2 (nombre minimum de cartes nécessaire à l'utilisation des fonctions d'administration) est recommandée. Les codes PIN de ces cartes doivent être suffisamment complexes.

OE15. Authentification_Mutuelle

Un module externe à la TSF doit permettre d'effectuer une authentification mutuelle entre la TOE et les utilisateurs (S1.Application_cliente, S2.Super-Administrateur_de_sécurité, S3.Administrateur_de_sécurité, S4.Gestionnaire_de_la_TOE, S5.Super-Gestionnaire_de_la_TOE) afin de se protéger contre l'usurpation d'identité.

OE16. Protection_Clé_Signature_Configuration

La clé privée utilisée pour la signature du fichier de configuration doit être protégée de manière adéquate, par exemple au travers d'une protection supérieure à celle des clés privées utilisées lors de l'authentification mutuelle

OE17. Protection_communications

Les communications entre la TOE et les utilisateurs (S1.Application_cliente, S2.Super-Administrateur_de_sécurité, S3.Administrateur_de_sécurité, S4.Gestionnaire_de_la_TOE, S5.Super-Gestionnaire_de_la_TOE) doivent être chiffrées par un module externe à la TSF, afin de protéger les communications en confidentialité. La protection doit être implémentée conformément aux recommandations de la DCSSI [CRYPT_STD].

OE18. Services_Tiers_De_Confiance

Les OCSP, IGC et serveurs d'horodatage auxquels la TOE fait une requête doivent fournir des informations considérées fiables.

6. EXIGENCES DE SECURITE

6.1 Exigences fonctionnelles de sécurité de la TOE

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

- *Raffiné éditorialement* (terme défini dans la [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 éditorial*: 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.

Les composants FDP_MRU.1 (§9.2) et FPT_TDI.1 (§9.3) étendent la partie 2 des Critères Communs.

6.1.1 Audit des actions des super-administrateurs

FAU_GEN.1/Super-Administrator actions audit Audit data generation

FAU_GEN.1.1/Super-Administrator actions audit The TSF shall be able to generate an audit record of the following auditable events:

- Start-up and shutdown of the audit functions;
- All auditable events for the **not specified** level of audit; and
- **Modification of the configuration by the super-administrator**.

FAU_GEN.1.2/Super-Administrator actions audit The TSF shall record within each audit record at least the following information:

- Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
- For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **none**.

Refinement:

Only configuration modifications committed by the administrator are audited.

Le niveau de détail et de profondeur des pistes d'audit (« *level of audit* ») est *not specified* car il n'y a qu'un seul niveau de détail dans les actions enregistrées dans les pistes.

FAU_GEN.2/Super-Administrator actions audit User identity association

FAU_GEN.2.1/Super-Administrator actions audit [Raffiné éditorialement] The TSF shall be able to associate each auditable event with the identity of the ~~user~~ **super-administrator** that caused the event.

Refinement:

Audit is only applied on administrator's configuration modifications.

FAU_SAR.1/Super-Administrator actions audit Audit review

FAU_SAR.1.1/Super-Administrator actions audit The TSF shall provide **super-administrators** with the capability to read **all audit information** from the audit records.

FAU_SAR.1.2/Super-Administrator actions audit [Raffiné éditorialement] The TSF shall provide the audit records in a manner suitable for the ~~user~~ **super-administrator** to interpret the information.

FAU_STG.1/Super-Administrator actions audit Protected audit trail storage

FAU_STG.1.1/Super-Administrator actions audit The TSF shall protect the stored audit records from unauthorised deletion.

FAU_STG.1.2/Super-Administrator actions audit The TSF shall be able to **detect** unauthorised modifications to the audit records in the audit trail.

6.1.2 Audit des actions des administrateurs

FAU_GEN.1/Administrator actions audit Audit data generation

FAU_GEN.1.1/Administrator actions audit The TSF shall be able to generate an audit record of the following auditable events:

- Start-up and shutdown of the audit functions;
- All auditable events for the **not specified** level of audit; and
- **Modification of the configuration by the administrator.**

FAU_GEN.1.2/Administrator actions audit The TSF shall record within each audit record at least the following information:

- Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
- For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **none**.

Refinement:

Only configuration modifications committed by the administrator are audited.

Le niveau de détail et de profondeur des pistes d'audit (« *level of audit* ») est *not specified* car il n'y a qu'un seul niveau de détail dans les actions enregistrées dans les pistes.

FAU_GEN.2/Administrator actions audit User identity association

FAU_GEN.2.1/Administrator actions audit [Raffiné éditorialement] The TSF shall be able to associate each auditable event with the identity of the ~~user~~ **administrator** that caused the event.

Refinement:

Audit is only applied on administrator's configuration modifications.

FAU_SAR.1/Administrator actions audit Audit review

FAU_SAR.1.1/Administrator actions audit The TSF shall provide **administrators** with the capability to read **all audit information** from the audit records.

FAU_SAR.1.2/Administrator actions audit [Raffiné éditorialement] The TSF shall provide the audit records in a manner suitable for the ~~user~~ **administrator** to interpret the information.

FAU_STG.1/Administrator actions audit Protected audit trail storage

FAU_STG.1.1/Administrator actions audit The TSF shall protect the stored audit records from unauthorised deletion.

FAU_STG.1.2/Administrator actions audit The TSF shall be able to **detect** unauthorised

modifications to the audit records in the audit trail.

FAU_SAR.2/Restricted Audit review

FAU_SAR.2.1/Restricted audit review The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

Refinement:

Audit records can only be reviewed by administrators.

6.1.3 Contrôles 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 ~~verifier~~client application,**
- **information: a signed document**
- **operation: import of the document in the TSC.**

FDP_IFF.1/Document acceptance Simple security attributes

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

- **subjects: the ~~verifier~~client application (signature policy),**
- **information: the signed document (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 "not checked".**

FDP_IFF.1.3/Document acceptance The TSF shall enforce the **none.**

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

- **capability to invoke an ~~external~~ internal checker in charge of controlling that the semantics of the document to be signed is invariant**
- **capability to inform the ~~verifier~~ client application when the document's semantics is not stable or not checked.**

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

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

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

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

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

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

Raffinement non édiorial:

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

FMT_MSA.3/Document's acceptance Static attribute initialisation

FMT_MSA.3.1/Document's acceptance The TSF shall enforce the **document acceptance 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.

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

FMT_MSA.1.1/Document's semantics invariance status [Raffiné éditorialement] The TSF shall enforce the **document acceptance information flow control policy** to restrict the ability to **modify** the security attribute **document's stability status** to **nobody**.

FMT_SMF.1/Getting document's semantics invariance status Specification of management functions

FMT_SMF.1.1/Getting document's semantics invariance status The TSF shall be capable of performing the following security management functions:

- **invoking an ~~external~~ internal module to get the status indicating whether the document's semantics is invariant or not.**

6.1.4 Présentation du document signé

FMT_MTD.1/Document format/viewer association table Management of TSF data

FMT_MTD.1.1/Document format/viewer association table The TSF shall restrict the ability to **modify** the **document format/viewer association table** to the **administrator**.

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

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

- **an administrator of the TOE shall be permitted to manage the document format/viewer association table.**

FMT_MTD.1/Viewer activation parameter Management of TSF data

FMT_MTD.1.1/Viewer activation parameter The TSF shall restrict the ability to **initialize** the **viewer activation parameter** to the **administrator**.

Raffinement global:

This configuration parameter initialization shall be performed upon the TOE installation.

FMT_SMF.1/Management of the viewer activation parameter Specification of management functions

FMT_SMF.1.1/Management of the viewer activation parameter The TSF shall be capable of performing the following security management functions:

- **the TOE installation procedure shall include the initialization the viewer activation parameter.**

6.1.5 Configuration

6.1.5.1 Gestion de l'ensemble des politiques de signature

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

FMT_MTD.1.1/Set of signature policies [Raffiné éditorialement] The TSF shall restrict the ability to **add and remove signature policies** to the **administrator**.

FMT_SMF.1/Management of the signature policies set Specification of management functions

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

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

6.1.5.2 Gestion des utilisateurs

Nota Bene : le terme « *operator* » désigne un « gestionnaire » (voir section 3.1.1, p. 14).

FMT_MTD.1/Super-Administrator-Set of authorized users Management of TSF data

FMT_MTD.1.1/Super-Administrator-Set of authorized users The TSF shall restrict the ability to **add and remove authorized super-administrators, administrators, super-operators and operators** to the **super-administrator**.

FMT_SMF.1/Super-Administrator-Management of authorized users set Specification of management functions

FMT_SMF.1.1/Super-Administrator-Management of authorized users set The TSF shall be capable of performing the following security management functions:

- **the super-administrator shall be permitted to add and remove super-administrators, administrators, super-operators and operators to/from the set of users that are authorized to connect to the TOE.**

FMT_MTD.1/Administrator-Set of authorized users Management of TSF data

FMT_MTD.1.1/Administrator-Set of authorized users The TSF shall restrict the ability to **add and remove authorized administrators and operators belonging to his group** to the **administrator**.

FMT_SMF.1/Administrator-Management of authorized users set Specification of management functions

FMT_SMF.1.1/Administrator-Management of authorized users set The TSF shall be capable of performing the following security management functions:

- **the administrator shall be permitted to add and remove administrators and operators to/from the set of users belonging to his group that are authorized to connect to the TOE.**

6.1.5.3 Gestion des applications autorisées

FMT_MTD.1/Set of authorized applications Management of TSF data

FMT_MTD.1.1/Set of authorized applications The TSF shall restrict the ability to **add and remove authorized applications** to the **administrator**.

FMT_SMF.1/Management of authorized applications set Specification of management functions

FMT_SMF.1.1/Management of authorized applications set The TSF shall be capable of performing the following security management functions:

- **the administrator shall be permitted to add and remove applications to/from the set of applications that are authorized to connect to the TOE.**

6.1.5.4 Sélection des ressources accessibles

FMT_MTD.1/Client application/trust policies association table Management of TSF data

FMT_MTD.1.1/Client application/trust policies association table The TSF shall restrict the ability to **modify the client application/trust policies association table** to the **administrator**.

FMT_SMF.1/Management of client application/trust policies association table Specification of management functions

FMT_SMF.1.1/Client application/trust policies association table The TSF shall be capable of performing the following security management functions:

- **the administrator shall be permitted to manage the client application/trust policies association table.**

FMT_MTD.1/Set of Resources Management of TSF data

FMT_MTD.1.1/Resources The TSF shall restrict the ability to **add and remove resources** to

the **super-administrator**.

Note : ces ressources sont les serveurs d'horodatage, les serveurs OCSP, les autorités de certification référencées…

FMT_SMF.1/Management of resources set Specification of management functions

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

- **the super-administrator shall be permitted to add and remove resources.**

6.1.5.5 Sélection de la politique de signature à appliquer

FMT_MTD.1/Selection of the applied signature policy Management of TSF data

FMT_MTD.1.1/Selection of the applied signature policy The TSF shall restrict the ability to **select** the **applied signature policy** to the ~~**verifier**~~ **client application**.

FMT_SMF.1/Selection of the applied signature policy Specification of management functions

FMT_SMF.1.1/Selection of the applied signature policy The TSF shall be capable of performing the following security management functions:

- **the ~~verifier~~ client application shall be permitted to select the signature policy to be applied.**

6.1.5.6 Protection des données de configuration

Ce composant (décrit en 9.3) étend la partie 2 des Critères Communs.

FPT_TDI.1/ Configuration data integrity TSF data integrity testing

FPT_TDI.1.1/Configuration data integrity The TSF shall be able **during initial start-up** to detect **modification** of **the configuration**.

FPT_TDI.1.2/Configuration data integrity Upon detection of a **configuration** data integrity error, the TSF shall take the following actions: **warn the administrator**.

Raffinement:

Il est précisé dans l'élément fonctionnel FPT_TDI.1.2 que la détection d'erreur se fait sur les données de configuration.

6.1.6 Rapports de services

FMT_MTD.1/Service report review Management of TSF data

FMT_MTD.1.1/Service report review The TSF shall restrict the ability to **review** the **service report** to the **operator**.

FMT_SMF.1/Service report review Specification of management functions

FMT_SMF.1.1/Service report review The TSF shall be capable of performing the following security management functions:

- **the operator shall be permitted to review service reports.**

FMT_MTD.1/Transactions review Management of TSF data

FMT_MTD.1.1/Transactions review The TSF shall restrict the ability to **review the transactions data** to the **operator**.

FMT_SMF.1/Transactions review Specification of management functions

FMT_SMF.1.1/Transactions review The TSF shall be capable of performing the following security management functions:

- **the operator shall be permitted to review the transactions data.**

6.1.7 Vérification de la signature

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

6.1.7.1 Import de la signature électronique et des attributs signés

Les exigences qui suivent se rapportent à l'import la signature électronique et aux attributs signés.

FDP_IFC.1/Electronic signature Subset information flow control

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

- **subjects: the ~~verifier~~ the client application,**
- **information: the signature and related signed attributes, and the signed document**
- **operation: import (i.e. acceptance as signed attributes conforming to the signature policy).**

Note d'application

Authorizing the import the electronic signature and related signed attributes means that signed attributes meet the rules defined in the applied signature policy.

FDP_IFF.1/Electronic signature Simple security attributes

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

- **subjects: the ~~verifier~~ the client application (applied signature policy)**
- **information: electronic signature (the signed attributes (signer's certificate reference, signature policy, commitment type, signer's role, signature's date and time, signature's location) and the signed document (the signed document's content format)).**

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

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

FDP_IFF.1.3/Electronic signature The TSF shall enforce the **none**.

FDP_IFF.1.4/Electronic signature The TSF shall provide the following

- **capability to launch the document viewer corresponding to the document's format, according to the document format/viewer association table, if the viewer activation parameter is set;**
- **capability to invoke an ~~external~~ internal module to check the invariance of the document's semantics;**
- **capability to inform the ~~verifier~~ the client application if the referenced signature policy is not the applied signature policy, when the electronic signature includes a reference to a signature policy.**

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

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

Note d'application (FDP_IFF.1.4) : l'activation de la visualisation (*viewer activation parameter*) est contrôlée au niveau des politiques de confiance par les administrateurs de la TOE.

Les applications de visualisation (*document viewer*) lancées par la TOE sont les navigateurs utilisés par les gestionnaires pour consulter les transactions effectuées.

Remarque : Le composant FDP_MRU.1 (décrit en 9.2) étend la partie 2 des Critères Communs.

FDP_MRU.1/Signed attributes Mandatory rules

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

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

- **if the signed attribute "signature policy" is present in the electronic signature, then its value is conformant to the signature policy;**
- **if the signed attribute "commitment type" is present in the electronic signature, then its value is conformant to the signature policy;**
- **if the signed attribute "claimed role" is present in the electronic signature, then its value is conformant to the signature policy;**
- **if the signed attribute "presumed signature date and time" is present in the electronic signature, then its value is conformant to the signature policy;**
- **if the signed attribute "presumed signature location" is present in the**

electronic signature then its value is conformant to the signature policy.

FMT_MSA.3/Electronic signature Static attribute initialisation

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

FMT_MSA.3.2/Electronic signature [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/Electronic signature Management of security attributes

FMT_MSA.1.1/Electronic signature The TSF shall enforce the **electronic signature information flow control policy** to restrict the ability to **modify** the security attributes **signature and its signed attributes** to **nobody**.

FDP_ITC.2/Electronic signature Import of user data with security attributes

FDP_ITC.2.1/Electronic signature The TSF shall enforce the **electronic signature information flow control policy** when importing user data, controlled under the SFP, from outside of the TSC.

FDP_ITC.2.2/Electronic signature The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3/Electronic signature The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4/Electronic signature The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5/Electronic signature The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: **none**

- **invoque an ~~external~~ internal module in charge of controlling the document's semantic invariance (using 1/ the signed document's content format provided by the electronic signature and 2/ the documents' content itself).**
- **transmit the result of the module's analysis to the ~~verifier~~ client application.**

6.1.7.2 Import d'une référence de temps valide

FDP_IFC.1/Time reference Subset information flow control

FDP_IFC.1.1/Time reference The TSF shall enforce the **time reference acceptance information flow control policy** on

- **subjects: the ~~verifier~~ the client application,**
- **information: the time reference applied to the signature**
- **operation: import of the time reference.**

Note d'application

Authorizing the export of certificates and related validation data means that the path is acceptanced as a valid certification path according to the signature policy.

FDP_IFF.1/Time reference Simple security attributes

FDP_IFF.1.1/Time reference The TSF shall enforce the **time reference acceptance information flow control policy** based on the following types of subject and information security attributes:

- **subjects: the ~~verifier~~ client application (applied signature policy)**
- **information: the time reference applied to the signer's numeric signature (attributes: the root keys applicable to verify the time-stamp tokens, time-stamp unit certificate, any needed certificate between the certificate and the root key).**

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

Operation: import of the time reference applied to the signer's numeric signature:

- **the key usage of the time-stamping unit certificate indicates that this certificate is only usable for time stamping purposes**
- **there exists a certification path between the time-stamping unit certificate and a root certificate dedicated to the verification of time-stamping tokens**
- **each rule applied to the previously mentioned certification path defined in requirement FDP_MRU.1/Certification path is met for the date/time included in the time reference, except the ones that are not explicitly referenced in the *applied signature policy*.**

FDP_IFF.1.3/Time reference The TSF shall enforce the **none**.

FDP_IFF.1.4/Time reference The TSF shall provide the following **none**.

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

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

FMT_MSA.3/Time reference Static attribute initialisation

FMT_MSA.3.1/Time reference The TSF shall enforce the **time reference acceptance information flow control policy** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/Time reference [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/Time reference Management of security attributes

FMT_MSA.1.1/Time reference The TSF shall enforce the **time reference acceptance information flow control policy** to restrict the ability to **modify** the security attributes **of the time reference** to **nobody**.

FDP_ITC.2/Time reference Import of user data with security attributes

FDP_ITC.2.1/Time reference The TSF shall enforce the **time reference acceptance information flow control policy** when importing user data, controlled under the SFP, from outside of the TSC.

FDP_ITC.2.2/Time reference The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3/Time reference The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4/Time reference The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5/Time reference The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: **none**.

6.1.7.3 Import d'un chemin de certification valide

Les exigences qui suivent se rapportent aux règles de vérification s'appliquant aux certificats d'un chemin de certification et permettant à l'application de déterminer si le chemin est valide ou non.

Certificats

FMT_MSA.1/Certificates Management of security attributes

FMT_MSA.1.1/Certificates The TSF shall enforce the **certification path acceptance information flow control policy** to restrict the ability to **modify** the security attributes **of the imported certificates** to **nobody**.

Données de validation des certificats

FMT_MSA.1/Certificates' validation data Management of security attributes

FMT_MSA.1.1/Certificates' validation data The TSF shall enforce the **certification path acceptance information flow control policy** to restrict the ability to **modify** the security attributes **of the certificates' revocation data** to **nobody**.

Divers

FDP_IFC.1/Certification path Subset information flow control

FDP_IFC.1.1/Certification path The TSF shall enforce the **certification path acceptance information flow control policy** on

- **subjects: the ~~verifier~~ the client application,**
- **information:**
  - **the certificates belonging to a certification path**
  - **the revocation data needed to validate the certification path**
- **operation: import of the information (i.e. meaning that the path is accepted as a valid certification path according to the signature policy).**

Note d'application

Authorizing the export of certificates and related validation data means that the path is accepted as a valid certification path according to the signature policy.

FDP_IFF.1/Certification path Simple security attributes

FDP_IFF.1.1/Certification path The TSF shall enforce the **certification path acceptance information flow control policy** based on the following types of subject and information security attributes:

- **subjects: the ~~verifier~~ the client application (applied signature policy)**
- **information: certification path validation data, including:**
  - **the certificates belonging to the certification path (certificates' fields)**
  - **the revocation data of each certificate in the certification path (revocation data's numeric signature, revocation data's revocation list).**

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

Import of the certification path components and related validation data:

- **the certification path binds the signer's certificate to a root certificate defined in the applied signature policy,**
- **each rule defined in requirement *FDP_MRU.1/Certification path* is met at the date/time included in the imported time reference, except the ones that are not explicitly referenced in the *applied signature policy***
- **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/Certification path The TSF shall enforce the **none**.

FDP_IFF.1.4/Certification path The TSF shall provide the following **none**.

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

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

Remarque : Le composant FDP_MRU.1 (décrit en 9.2) étend la partie 2 des Critères Communs.

FDP_MRU.1/Certification path Mandatory rules

FDP_MRU.1.1/Certification path The TSF shall be able to apply a set of rules in enforcing the **certification path acceptance information flow control policy and the time reference information flow control policy**.

FDP_MRU.1.2/Certification path The TSF shall be able to apply the following set of rules

- **for each certificate of the certification path, the numeric signature of the certificate is correct**
- **for each certificate of the certification path, the period of validity of the certificate includes the date included in the time reference**
- **for each revocation data, the numeric signature of the revocation data is correct**
- **for each certificate of the certification path, the certificate is not revocated at the date included in the time reference**
- **for each certificate of the certification path, except the leaf certificate, the key usage indicate that the certificate is a CA certificate**
- **for each certificate of the certification path, the certification policy is conformant with the applied signature policy (application note: there may be different requirements for the CA certificates and for the leaf certificate).**

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 **electronic signature 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 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).**

FMT_MSA.3/Certification path Static attribute initialisation

FMT_MSA.3.1/Certification path The TSF shall enforce the **certification path acceptance information flow control policy** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/Certification path [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.2/Certification path Import of user data with security attributes

FDP_ITC.2.1/Certification path The TSF shall enforce the **certification path acceptance information flow control policy** when importing user data, controlled under the SFP, from outside of the TSC.

FDP_ITC.2.2/Certification path The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3/Certification path The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4/Certification path The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5/Certification path The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC:

- **a valid time reference has been imported (see *FDP_IFC.1/Time reference* and associated requirements), in conformance to the applied signature policy;**
- **any data needed to control certificates non repudiation have been imported, in conformance to the applied signature.**

6.1.7.4 Capacité à interpréter les données importées

Les exigences qui suivent porte sur la capacité de la TOE à interpréter les données importées.

FPT_TDC.1/Electronic signature Inter-TSF basic TSF data consistency

FPT_TDC.1.1/Electronic signature The TSF shall provide the capability to consistently interpret **the electronic signature** when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/Electronic signature The TSF shall use **the following standards:**

- PKCS #7
- CMS
- PDF
- XML-DSig
- XAdES (versions 1.2.2 and 1.3.2)

when interpreting the TSF data from another trusted IT product.

FPT_TDC.1/Time reference Inter-TSF basic TSF data consistency

FPT_TDC.1.1/Time reference The TSF shall provide the capability to consistently interpret **time references** when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/Time reference The TSF shall use the following standard:

- RFC 3161

when interpreting the TSF data from another trusted IT product.

FPT_TDC.1/Certificates Inter-TSF basic TSF data consistency

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

FPT_TDC.1.2/Certificates The TSF shall use the following standards:

- PKCS #6
- PKCS #10
- RFC 3280
- RFC 3739

when interpreting the TSF data from another trusted IT product.

FPT_TDC.1/Certificate revocation data Inter-TSF basic TSF data consistency

FPT_TDC.1.1/Certificate revocation data The TSF shall provide the capability to consistently interpret **certificates' revocation data** when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/Certificate revocation data The TSF shall use the following standards:

- RFC 3280

when interpreting the TSF data from another trusted IT product.

6.1.7.5 Retour du statut de vérification de signature

FDP_IFC.1/Electronic signature validation Subset information flow control

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

- **subject: the ~~verifier~~ client application**
- **information: validation status "correct signature"**
- **operations: communication of the status to the ~~verifier~~ client application.**

FDP_IFF.1/Electronic signature validation Simple security attributes

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

- **subject: the ~~verifier~~ client application (the signed document)**
- **information: validation status "correct signature" (signer's public key, document's hash, document's numeric signature).**

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

Communication of the status to the ~~verifier~~ client application:

- **there exists a valid certification path binding the signer's certificate to a root certificate referenced in the applied signature policy and therefore authenticating the signer's public key;**
- **the document's numeric signature, verified using the signer's public key, is correct.**

FDP_IFF.1.3/Electronic signature validation The TSF shall enforce the **none**.

FDP_IFF.1.4/Electronic signature validation The TSF shall provide the following

- **capability to communicate the status "wrong signature" if at least one rules among the information control policy rules is false.**

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

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

FMT_MSA.3/Signature validation status Static attribute initialisation

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

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

FMT_MSA.1/Signature validation status Management of security attributes

FMT_MSA.1.1/Signature validation status The TSF shall enforce the **electronic signature validation information flow policy** to restrict the ability to **modify** the security attributes **signature validation status** to **nobody**.

FDP_ETC.2/Verification status Export of user data with security attributes

FDP_ETC.2.1/Verification status The TSF shall enforce the **electronic signature validation information flow policy** when exporting user data, controlled under the SFP(s), outside of the TSC.

FDP_ETC.2.2/Verification status The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3/Verification status The TSF shall ensure that the security attributes, when exported outside the TSC, are unambiguously associated with the exported user data.

FDP_ETC.2.4/Verification status The TSF shall enforce the following rules when user data is exported from the TSC:

- **data exported as security attributes of the verification status are:**

- **the validation data contributing to prove the verification status correctness,**
- **the signed attributes,**
- **the limit on the value of transactions for which the signer's certificate can be used, if it is specified in the signer's certificate, and**
- **the result of the analysis of the document's semantics invariance to the verifier.**
- **the content of the signed document**

Note d'application

Les données de validation sont destinées à être éventuellement réutilisées lors d'une vérification ultérieure.

Les attributs signés, la limitation sur le montant de la transaction et la stabilité de la sémantique du document sont communiqués ~~au vérificateur~~ à l'application cliente par une interface programmatique ou une interface homme/machine.

6.1.7.6 Retour du statut de validation de certificat

FDP_IFC.1/Certificate validation Subset information flow control

FDP_IFC.1.1/Certificate validation The TSF shall enforce the **certificate validation information flow policy** on

- **subject: the client application**
- **information: validation status "valid certificate"**
- **operations: communication of the status to the client application.**

FDP_IFF.1/Certificate validation Simple security attributes

FDP_IFF.1.1/Certificate validation The TSF shall enforce the **certificate validation information flow policy** based on the following types of subject and information security attributes:

- **subject: the client application (the certificate)**
- **information: validation status "valid certificate" (certificate's public key, certificate's numeric signature).**

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

Communication of the status to the client application:

- **there exists a valid certification path binding the certificate to a root certificate referenced in the applied signature policy and therefore authenticating the certificate's public key;**

FDP_IFF.1.3/Certificate validation The TSF shall enforce the **none**.

FDP_IFF.1.4/Certificate validation The TSF shall provide the following

- **capability to communicate the status "invalid certificate" if at least one rule among the information control policy rules is false.**

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

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

FMT_MSA.3/Certificate validation status Static attribute initialisation

FMT_MSA.3.1/Certificate validation status The TSF shall enforce the **certificate validation information flow policy** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/Certificate validation status 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/Certificate validation status Management of security attributes

FMT_MSA.1.1/Certificate validation status The TSF shall enforce the **certificate validation information flow policy** to restrict the ability to **modify** the security attributes **certificate validation status** to **nobody**.

FDP_ETC.2/Certificate validation status Export of user data with security attributes

FDP_ETC.2.1/Certificate validation status The TSF shall enforce the **certificate validation information flow policy** when exporting user data, controlled under the SFP(s), outside of the TSC.

FDP_ETC.2.2/Certificate validation status The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3/Certificate validation status 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/Certificate validation status The TSF shall enforce the following rules when user data is exported from the TSC:

- **data exported as security attributes of the validation status are:**
  - **the validation data contributing to prove the validation status correctness,**

- o **and the content of the certificate**

Note d'application

Les données de validation sont destinées à être éventuellement réutilisées lors d'une vérification ultérieure.

6.1.8 Support cryptographique

FCS_COP.1/Signature verification Cryptographic operation

FCS_COP.1.1/Signature verification The TSF shall perform **numeric signature verification** in accordance with a specified cryptographic algorithm

- **RSA**

and cryptographic key sizes

- **Belonging to the following list: 1024, 1536, 2048, 3072, 4096 or 8192 bits**

that meet the following: **[CRYPT-STD]**, [PKCS #1].

FCS_COP.1/Hash Cryptographic operation

FCS_COP.1.1/Hash The TSF shall perform

- **hash generation**

in accordance with a specified cryptographic algorithm

- **SHA-1**
- **SHA-256**
- **SHA-384**
- **SHA-512**

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

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

Refinement:

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

6.1.9 Identification et authentification des utilisateurs

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles

- ~~**verifier**~~ **the client application**
- **administrator**
- **super-administrator**
- super-operator
- **operator**

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

Rappel : Le terme « *operator* » désigne les gestionnaires de la TOE et non l'opérateur d'hébergement (qui n'est pas un rôle de la TOE).

FIA_UID.2 User identification before any action

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

FIA_UAU.1/(Super-)Administrator authentication Timing of authentication

FIA_UAU.1.1/(Super-)Administrator authentication [Raffiné éditorialement] The TSF shall allow **any actions** on behalf of the user to be performed before the user is authenticated, **except the following administration operations**:

- **Management of the viewer activation parameter**
- **Management of the document format/viewer association table**
- ~~**Management**~~ **Modification of the signature policies set**
- **Modification of authorized users set**
- **Modification of resources set**
- **Modification of authorized applications set**
- **Modification of the client application/trust policies association table**
- **Consultation of the audit trails**

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

Note :

Cette authentification est réalisée au travers de la signature par le super-administrateur ou l'administrateur du nouveau fichier de configuration pour toutes les opérations de modification de la configuration, et par certificat SSL pour ce qui est de la consultation des pistes d'audit.

6.2 Exigences d'assurance

Le niveau des exigences de sécurité d'assurance est EAL3. L'EAL a été augmenté avec ADV_IMP.1 (pour FCS seulement, c'est-à-dire les algorithmes cryptographiques implantés dans la TOE), ADV_LLD.1 (pour FCS seulement), ALC_FLR.3, ALC_TAT.1 (pour FCS seulement) et AVA_VLA.2.

7. SPECIFICATIONS GLOBALES DE LA CIBLE D'EVALUATION

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

7.1 Fonctions de sécurité de la cible d'évaluation

7.1.1 F.Validation_Signature

Cette fonction permet à une application d'effectuer une demande de validation de signature au serveur DVS, au travers d'une interface d'appel de type Web Services.

Le module externe d'authentification se charge d'authentifier l'application par certificat au travers du protocole SSLv3 avec authentification mutuelle.

La TOE reçoit la requête de vérification et récupère le certificat avec lequel l'application s'est authentifiée (SSLv3) auprès du module externe d'authentification.

Elle effectue alors une vérification complète du certificat d'authentification de l'application.

Une fois cette vérification effectuée, elle utilise le certificat d'application pour s'assurer que l'application est bien déclarée comme autorisée dans la configuration DVS.

Elle récupère dans la requête l'identifiant de transaction, qui, associé au certificat de l'application appelante, lui permet d'identifier de manière non ambiguë la Politique de Confiance à appliquer.

Elle applique ensuite cette Politique de Confiance :

- Identification du format de signature :
- Horodatage de réception afin de fixer la signature dans le temps.
- Vérification cryptographique de la signature.
- Extraction du document signé et contrôle de sa stabilité sémantique.
- Vérification de la conformité des propriétés de la signature par rapport aux éléments paramétrés dans la Politique de Confiance
    - Cohérence temporelle. Il s'agit ici de s'assurer du respect du décalage autorisé entre la date de signature déclarée et la date courante.
    - Rôle déclaré du signataire.
    - Lieu déclaré de signature (comprenant la ville, le code postal et le pays)
    - (Une référence à la) Politique de signature, identifiée par son OID et son empreinte, telle qu'incluse dans les attributs de la signature.
    - Type d'engagement endossé par le signataire :
- Validation du ou des jetons d'horodatage présents dans la signature reçue.
- Validation des certificats de signature.
- Création, signature et horodatage de la preuve de validation
- Archivage de la preuve de validation

La réponse à la requête de validation, contenant la preuve générée, est alors retournée à l'application appelante.

7.1.2 F.Validation_Certificat

Cette fonction permet à une application d'effectuer une demande de validation de certificat au serveur DVS, au travers d'une interface d'appel de type Web Services.

Le module externe d'authentification se charge d'authentifier l'application par certificat au travers du protocole SSLv3 avec authentification mutuelle.

La TOE reçoit la requête de vérification et récupère le certificat avec lequel l'application s'est authentifiée (SSLv3) auprès du module externe d'authentification.

Elle effectue alors une vérification complète du certificat d'authentification de l'application.

Une fois cette vérification effectuée, elle utilise le certificat d'application pour s'assurer que l'application est bien déclarée comme autorisée dans la configuration DVS.

Elle récupère dans la requête l'identifiant de transaction, qui, associé au certificat de l'application appelante, lui permet d'identifier de manière non ambiguë la Politique de Confiance à appliquer.

Elle applique ensuite cette Politique de Confiance :

- Validation du certificat
  - Contrôle d'appartenance à une liste blanche de certificats / de DN
  - Construction et validation de la chaîne de certification
  - Vérification des extensions du certificat
- Création, signature et horodatage de la preuve de validation
- Archivage de la preuve de validation

La réponse à la requête de validation, contenant la preuve générée, est alors retournée à l'application appelante.

7.1.3 F.Génération_Audit

Cette fonction génère une trace d'audit pour chacun des événements suivants :

- Démarrage de la TOE
- Modifications de configuration effectuée par les super-administrateurs et par les administrateurs

Pour chaque événement, elle enregistre l'heure et la date de l'événement, l'identité de l'utilisateur et la réussite ou l'échec de l'événement (dans le cas d'une modification de configuration).

Ces traces sont générées et enregistrées lorsque la configuration est effectivement modifiée (sauvegardée) par un administrateur ou un super-administrateur : comme décrit en 3.2.2.4, les administrateurs et super-administrateurs travaillent sur une copie « locale » de la configuration sur leur poste de travail. Ces modifications ne sont prises en compte par qu'une fois signées et validée par la TOE lorsqu'ils les sauvegardent ; les pistes ne contiennent que les modifications prises en compte par la TOE.

Chaque fichier d'audit est signé afin de détecter une modification de celui-ci. Cette signature est effectuée par le HSM (hors-TOE).

7.1.4 F.Gestionnaires

Cette interface permet aux gestionnaires d'effectuer des opérations de :

- Recherche d'une transaction
- Récupération d'une preuve

- Consulter des rapports d'activité
- Visualiser les données signées contenues dans une preuve

Sur les applications pour lesquelles ils sont autorisés. La visualisation des données signées n'est possible que si la configuration le permet et ne concerne que les documents au format « texte » ou « HTML » dont la sémantique a été validée.

7.1.5 F.Super-Gestionnaires

Cette interface permet aux super-gestionnaires d'effectuer des opérations suivantes sur toutes les applications :

- Recherche d'une transaction
- Récupération d'une preuve
- Consultation des rapports d'activité
- Visualiser les données signées contenues dans une preuve

La visualisation des données signées n'est possible que si la configuration le permet et ne concerne que les documents au format « texte » ou « HTML » dont la sémantique a été validée.

7.1.6 F.Super-Administration

Cette interface permet aux super-administrateurs d'effectuer des opérations de :

- Gestion des groupes d'administration d'application
- Définition des ressources mises à la disposition des administrateurs d'applications :
  - Paramétrage des clés de signature
  - Référencement des autorités de certification
  - Référencement des politiques de certification
  - Paramétrage des serveurs d'horodatage et OCSP
  - Configuration de services d'archivage externes
  - Définition de la liste des applications de visualisation pouvant être référencées dans une politique de confiance
- Consultation des pistes d'audit du serveur de confiance et vérification de leur signature

Bien qu'authentifié par l'environnement, cette fonction demande l'authentification du super-administrateur au travers de la signature par ce dernier du fichier de configuration, au moment de l'enregistrement de la nouvelle configuration.

7.1.7 F.Administration

Cette interface permet aux administrateurs d'effectuer des opérations de :

- Gestion des utilisateurs au sein de leur groupe
- Paramétrage des politiques de confiance mutualisées
- Ouverture du service à de nouvelles applications métiers
- Création de transactions pour une application donnée et association à chacune de ces transactions d'une politique de confiance
- Consultation des pistes d'audit relatives à leurs groupes respectifs et vérification de leur signature.

Bien qu'authentifié par l'environnement, cette fonction demande l'authentification de l'administrateur au travers de la signature par ce dernier du fichier de configuration, au moment de l'enregistrement de la nouvelle configuration.

7.2 Mesures d'assurance

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

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

7.2.1 Développement

7.2.1.1 Documents de développement et des outils de développement

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

Le premier niveau décrit les interfaces externes de la TOE, 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'applique qu'aux fonctions cryptographiques spécifiées au travers des exigences *FCS_COP.1/Signature verification* et *FCS_COP.1/Hash function*.

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

Les documents fournis pour répondre à ces mesures sont :

- Spécifications fonctionnelles,
- Architecture du produit,
- Architecture détaillée des fonctions cryptographiques,
- Code source des fonctions cryptographiques,
- Document de correspondance

Ces mesures d'assurance couvrent les exigences suivantes :

- ADV_FSP.1
- ADV_HLD.2
- ADV_LLD.1
- ADV_IMP.1
- ADV_RCR.1

7.2.2 Support au développement et livraison

7.2.2.1 Procédures de développement et outils de gestion de configuration

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

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

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

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

Le document fourni pour répondre à ces mesures est :

- Procédures de développement

Ces mesures d'assurance couvrent les exigences suivantes :

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

7.2.2.2 Procédures de correction d'anomalies

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

Le document fourni pour répondre à ces mesures est :

- Correction d'anomalies

Cette mesure d'assurance couvre l'exigence suivante :

- ALC_FLR.3

7.2.2.3 Procédure de livraison

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

Le document fourni pour répondre à ces mesures est :

- Procédure de livraison

Cette mesure d'assurance couvre l'exigence suivante :

- ADO_DEL.1

7.2.3 Tests et analyse de vulnérabilité

7.2.3.1 Documents de test

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

Le document fourni pour répondre à ces mesures est :

- Dossier de test

Ces mesures d'assurance couvrent les exigences suivantes :

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

7.2.3.2 Analyse de vulnérabilité

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

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

Le document fourni pour répondre à ces mesures est :

- Dossier d'analyse de vulnérabilité

Ces mesures d'assurance couvrent l'exigence suivante :

- AVA_VLA.2

7.2.4 Guides

7.2.4.1 Procédure d'installation et de démarrage

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

Le document fourni pour répondre à ces mesures est :

- Procédure d'installation

Cette mesure d'assurance couvre l'exigence suivante :

- ADO_IGS.1
- AVA_MSU.1

7.2.4.2 Guide pour le développement d'applications clientes

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

Le document fourni pour répondre à ces mesures est :

- Guide de développement d'applications

Cette mesure d'assurance couvre l'exigence suivante :

- AGD_ADM.1
- AVA_MSU.1

7.2.4.3 Guide pour le super-administrateur de la TOE

Un guide s'adressant aux super-administrateurs de la TOE décrit la manière d'utiliser les fonctions de sécurité du produit et leurs interfaces, accessibles aux super-administrateurs.

Le document fourni pour répondre à ces mesures est :

- Guide du super-administrateur

Cette mesure d'assurance couvre l'exigence suivante :

- AGD_ADM.1
- AVA_MSU.1

7.2.4.4 Guide pour l'administrateur de la TOE

Un guide s'adressant aux administrateurs de la TOE décrit la manière d'utiliser les fonctions de sécurité du produit et leurs interfaces, accessibles aux administrateurs.

Le document fourni pour répondre à ces mesures est :

- Guide de l'administrateur

Cette mesure d'assurance couvre l'exigence suivante :

- AGD_ADM.1
- AVA_MSU.1

7.2.4.5 Guide pour les gestionnaires et super-gestionnaires de la TOE

Un guide s'adressant aux gestionnaires et super-gestionnaires de la TOE décrit la manière d'utiliser les fonctions de sécurité du produit et leurs interfaces.

Le document fourni pour répondre à ces mesures est :

- Guide du gestionnaire et du super-gestionnaire

Cette mesure d'assurance couvre l'exigence suivante :

- AGD_ADM.1
- AVA_MSU.1

7.2.4.6 Guide pour le vérificateur (humain)

Un guide d'utilisation s'adressant aux vérificateurs humains (utilisateurs finaux) est disponible. Cependant, de part la nature même de la TOE, ce guide n'est disponible qu'au travers de l'application cliente. Il doit être intégré à la documentation de l'application cliente.

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

7.2.5 Couverture des mesures d'assurance

Composant d'assurance	Mesure d'assurance
ACM_CAP.3	§7.2.2.1
ACM_SCP.1	§7.2.2.1
ADO_DEL.1	§7.2.2.3
ADO_IGS.1	§7.2.4.1
ADV_FSP.1	§7.2.1.1
ADV_HLD.2	§7.2.1.1

Composant d'assurance	Mesure d'assurance
ADV_LLD.1	§7.2.1.1
ADV_IMP.1	§7.2.1.1
ADV_RCR.1	§7.2.1.1
AGD_ADM.1	§7.2.4.2 §7.2.4.3 §7.2.4.4 §7.2.4.5
AGD_USR.1	§7.2.4.6
ALC_DVS.1	§7.2.2.1
ALC_TAT.1	§7.2.2.1
ALC_FLR.3	§7.2.2.2
ATE_COV.2	§7.2.3.1
ATE_DPT.1	§7.2.3.1
ATE_FUN.1	§7.2.3.1
ATE_IND.2	§7.2.3.1
AVA_MSU.1	§7.2.4.1 §7.2.4.2 §7.2.4.3 §7.2.4.4 §7.2.4.5 §7.2.4.6
AVA_SOF.1	-
AVA_VLA.2	§7.2.3.2

8. CONFORMITE AU PROFIL DE PROTECTION

8.1 Référence du Profil de protection

La cible de sécurité est conforme au profil de protection « Module de vérification de signature électronique » [EXT_DCSSI_PP] pour les documents au format « texte brut » et HTML.

Voir la section 8.2.4 pour les détails.

8.2 Modifications apportées par rapport au Profil de protection

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

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

Les modifications sont présentées par « thème » (politique de signature, affichage, contrôle de sémantique, …). Un élément (hypothèse, menace, objectifs, …) peut faire partie de plusieurs « thèmes ».

8.2.1 Politique de signature et politiques de confiance

Dans le profil de protection, une **politique de signature** est définie comme « un ensemble de règles pour la création ou la validation d'une signature électronique, sous lesquelles une signature électronique peut être déterminée valide. » [EXT_DCSSI_PP, 2.2].

La TOE utilise quant à elle des **politiques de confiance** (3.1.2, p. 15). Ces politiques de confiance définissent les politiques de signatures au sens du profil (« Paramètres de validation de la signature »), mais aussi la façon dont sont vérifiés les certificats du signataire (« Paramètres de validation du certificat ») et les paramètres de constitution de la preuve (incluant elle-même des références à des politiques de signature, distinctes de celles de la signature soumise à la TOE par l'application appelante). Autrement dit, **les politiques de signature au sens du profil sont une partie des politiques de confiance de la TOE**.

Le terme « politique de confiance » est conservé dans ce document lorsque cela est nécessaire, par exemple dans les données de configuration du service (bien B14.Configuration_du_service), car c'est bien d'une politique de confiance dont il s'agit ici, et non des seules règles de validation de signature. Pareillement, dans la description des fonctions de sécurité (7.1, p.69), un certain nombre de vérifications et de choix effectués par la TOE (p. ex. détection du format de signature, génération de la preuve) sortent du strict cadre de la validation d'une signature ou d'un certificat. C'est pourquoi on trouvera parfois des abus de langage comme le fait que la TOE « applique une politique de confiance ».

Partout ailleurs, le terme « politique de signature » (ou « *signature policy* » dans les SFR) du profil a été conservé.

Concernant la sélection de la politique à appliquer [EXT_DCSSI_PP, 2.4.2], les politiques de confiance définissent (3.1.2.1 et 3.1.2.2, p. 15) des politiques de signature (ou de vérification) autorisées. Lorsqu'une application soumet une signature, on compare les (OID des) politiques éventuellement référencées dans celle-ci avec les (OID des) politiques autorisées (dans la politique de confiance) ; en cas d'incompatibilité, ce fait est remonté dans le statut de vérification renvoyé à l'application appelante. Par rapport au processus présenté dans le profil, la seule différence est que l'application cliente ne soumet pas directement la politique à appliquer : celle-ci est en effet sélectionnée par la TOE à partir de l'identifiant de transaction soumis par l'application (3.1.2, p. 15).

Le tableau ci-dessous présente la correspondance entre les éléments constitutifs d'une politique de signature au sens du profil de protection [EXT_DCSSI_PP, 2.2] et les éléments apparaissant dans une politique de confiance.

Élément d'une politique de signature d'après le profil de protection	Élément des politiques de confiance
L'identification d'un ou plusieurs points de confiance et des règles permettant de construire un chemin de certification entre le certificat du signataire et l'un de ces points de confiance.	Liste blanche de DN, liste des certificats autorisés et des AC autorisées (3.1.2.2)
Les moyens à mettre en œuvre pour obtenir une référence de temps destinée à positionner dans le temps la signature numérique du signataire (ex : horodatage)	Configuration des serveurs d'horodatage et OCSP (3.2.2.1)
Les moyens à utiliser pour vérifier le statut de révocation de chaque certificat du chemin de certification par rapport à cette référence de temps.	*Idem.*
Les caractéristiques que doit comporter le certificat du signataire (ex : OID de politique de certification, QCStatements, key usage, etc.).	Paramètres de validation d'un certificat (3.1.2.2), comme l'OID de la politique de signature, l'obligation que le certificat soit qualifié, etc.
Les types d'attributs qui, outre la référence au certificat du signataire, doivent être signés conjointement avec le document (ex : référence à une politique de signature, type d'engagement, date présumée de la signature numérique, format du document, rôle présumé du signataire, lieu présumé de la signature numérique, etc.).	Paramètres de validation d'une signature (3.1.2.1).
L'ensemble des données de validation que le signataire doit fournir.	Paramètres de validation d'une signature (3.1.2.1).
Les moyens à mettre en œuvre pour obtenir une référence de temps destinée à positionner dans le temps les données de validation (ex : horodatage).	Configuration des serveurs d'horodatage et OCSP (3.2.2.1)
Les algorithmes cryptographiques (signature et hachage) à utiliser dans le cadre de la vérification de la signature numérique du document et des données de validation.	Contenu dans les formats de signature attendus (3.1.3).

8.2.2 Les sujets

Des modifications sur les sujets ont été effectuées par rapport au profil de protection.

Le sujet *S.Vérificateur* a été supprimé pour être remplacé par S1.Application_cliente, afin d'apporter la précision dans l'ensemble de la cible de sécurité que la TOE est utilisée par une application et non un utilisateur humain (hormis pour les opérations d'administration et de supervision).

Le sujet *S2.Super-Administrateur_de_sécurité* a été ajouté. Il s'agit de l'administrateur « des administrateurs ». Il peut gérer tous les utilisateurs et les ressources accessibles (serveur d'horodatage, OCSP, autorité de certification référencées…).

Les sujets *S4.Gestionnaire_de_la_TOE* et *S5.Super-Gestionnaire_de_la_TOE* ont été ajoutés afin d'effectuer des opérations annexes : connaître le nombre de transactions effectuées et effectuer des recherches au sein des transactions effectuées.

Ces sujets ont donc été ajoutés au paragraphe 4.1.3 et au composant *FMT_SMR.1*.

Catégorie	Nom de l'élément	Modification apportée	Commentaires
Sujet	S.Vérificateur	Suppression du sujet	Le vérificateur est une application cliente. Afin de rendre explicite cet état, le sujet a été remplacé par S1

Catégorie	Nom de l'élément	Modification apportée	Commentaires
Sujet	S1.Application_cliente	Ajout des sujets	Remplace S.Vérificateur
Sujet	S2.Super-Administrateur_de_sécurité		Ce sujet effectue des opérations de « super-administration »
Sujet	S4.Gestionnaire_de_la_TOE S5.Super-Gestionnaire_de_la_TOE		Ce sujet effectue des opérations de gestion différentes de l'administrateur.
Exigence fonctionnelle	FMT_SMR.1	Ajout du rôle	Les rôles « operator » et « super-operator » ont été ajoutés.
		Précision	Le mot « verifier » est remplacé par « client application »

L'hypothèse (H4) concernant l'administrateur a été étendue (au travers de son intitulé) pour prendre en compte les super-administrateurs et dupliquée pour le gestionnaire afin de prendre en compte son ajout. Par ailleurs, le texte cette hypothèse a été complété afin de rappeler l'importance de la configuration par les administrateurs et super-administrateurs des politiques de signature et de validation de signature au sein de la TOE, ainsi que de leur rôle dans le maintien de la cohérence entre les OID référencées et la mise en œuvre des politiques correspondantes. De plus, comme l'application cliente est développée en dehors de la TOE, une hypothèse la concernant a été ajoutée.

Ajouter les super-administrateurs nécessite aussi d'étendre la menace *M1* pour prendre en compte les fonctionnalités de ces derniers.

Catégorie	Nom de l'élément	Modification apportée	Commentaires
Hypothèse	H4.(Super-)Administrateur_De_Sécurité_Sûr	Hypothèse étendue	Hypothèse étendue aux super-administrateurs et mention de la configuration de la TOE.
Hypothèse	H5.Gestionnaire_Sûr	Ajout des éléments	Même hypothèse que celle concernant l'administrateur « de confiance »
Hypothèse	H6.Application_Cliente_Sûre		Voir note
Menace	M1.Modification_Ens_Politiques_Signature	Menace étendue	Ajout des fonctionnalités des super-administrateurs
Objectif	OE6.(Super-)Administrateur_De_Sécurité_Sûr	Objectif étendu	Objectif étendu afin de couvrir l'hypothèse H4
Objectif	OE7.Gestionnaire_Sûr	Ajout des éléments	Afin de couvrir l'hypothèse H5
Objectif	OE8.Application_Cliente_Sûre		Afin de couvrir l'hypothèse H6

Note : Une application cliente se trouve entre l'utilisateur final (humain) et la TOE. C'est pourquoi elle doit être de confiance, tant vis-à-vis de la TOE car elle peut s'y connecter que vis-

à-vis de l'utilisateur puisqu'elle retranscrit le résultat de la vérification et doit au besoin faire appel à une application externe de présentation du document.

Enfin, les utilisateurs, les (super-)administrateurs et les gestionnaires accèdent à la TOE au travers de postes de travail. Au même titre que pour la machine hôte de la TOE, des hypothèses ont été formulée sur leurs postes :

Catégorie	Nom de l'élément	Modification apportée	Commentaires
Hypothèse	H2.Poste_(Super-)Administrateur	Ajout des éléments	Nous faisons quasiment les mêmes hypothèses sur le poste des (super-)administrateurs et des gestionnaires que sur la machine hôte de la TOE
Hypothèse	H3.Poste_Gestionnaire		
Objectif	OE3.Poste_(Super-)Administrateur		Afin de couvrir l'hypothèse H2
Objectif	OE4.Poste_Gestionnaire		Afin de couvrir l'hypothèse H3

8.2.3 Hypothèses ajoutées

Un certain nombre d'hypothèses ont été ajoutées sur l'environnement de la TOE, afin de prendre en compte son implémentation par rapport au produit « générique » présenté dans le profil de protection. Ainsi, on été ajoutées :

- Des hypothèses sur les journaux d'audit, car la TOE est installée sur un serveur.

Catégorie	Nom de l'élément	Modification apportée	Commentaires
Hypothèse	H11.Analyse_Périodique_journaux	Ajout des éléments	La TOE étant sur un serveur, on suppose que les administrateurs vérifient périodiquement les journaux afin de s'assurer du bon fonctionnement continu de la TOE
Hypothèse	H12.Suppression_Périodique_journaux		Ces mêmes journaux d'événements devront être supprimés régulièrement afin de ne pas saturer les disques de stockages
Objectif	OE11.Analyse_Périodique_Journaux		Afin de couvrir l'hypothèse H11
Objectif	OE12.Suppression_Périodique_journaux		Afin de couvrir l'hypothèse H12

- Des hypothèses sur les moyens d'authentification auprès de la TOE des administrateurs et des gestionnaires. En effet, une authentification mutuelle est

effectuée avant toute opération. Cette authentification est réalisée par un module externe à la TOE.

Catégorie	Nom de l'élément	Modification apportée	Commentaires
Hypothèse	H13.Protection_Moyens_Authentification	Ajout des éléments	Les moyens d'authentification doivent être protégés afin de prévenir une utilisation malveillante de l'accès d'administration et de supervision
Hypothèse	H15.Authentification_Mutuelle		Cette hypothèse permet de se protéger contre l'usurpation d'identité.
Objectif	OE13.Protection_Moyens_Authentification		Afin de couvrir l'hypothèse H13
Objectif	OE15.Authentification_Mutuelle		Afin de couvrir l'hypothèse H15

- Une hypothèse sur l'activation et l'administration du HSM afin de prévenir une utilisation ou une tentative d'accès malveillante.

Catégorie	Nom de l'élément	Modification apportée	Commentaires
Hypothèse	H14.Protection_HSM	Ajout des éléments	-
Objectif	OE14.Protection_HSM		Afin de couvrir l'hypothèse H14

- Une hypothèse concernant la clé de signature, car la modification de la configuration est réalisée au travers de la signature du nouveau fichier de configuration par un administrateur.

Catégorie	Nom de l'élément	Modification apportée	Commentaires
Hypothèse	H16.Protection_Clé_Signature_Configuration	Ajout des éléments	-
Objectif	OE16.Protection_Clé_Signature_Configuration		Afin de couvrir l'hypothèse H16

- Une hypothèse concernant la protection des communications entre le poste sur lequel se trouve l'application cliente et la TOE. Ces communications doivent essentiellement être protégées en intégrité.
  Bien que non obligatoire, car les données échangées entre l'application cliente et la TOE sont déjà protégées en intégrité – la requête de vérification de signature est faite sur un document signé et la réponse est signée par la TOE et contient le document signé qui vient d'être vérifié –, la protection de la communication assure toutefois une meilleure fiabilité de ces données échangées et permet à l'application cliente de ne pas vérifier la signature de la réponse.

Catégorie	Nom de l'élément	Modification apportée	Commentaires
Hypothèse	H17.Protection_Communications	Ajout des éléments	-
Objectif	OE17.Protection_communications		Afin de couvrir l'hypothèse H17

- Une hypothèse concernant les services tiers (serveurs OCSP, IGC et AC) qui suppose que les informations qu'ils transmettent sont fiables

Catégorie	Nom de l'élément	Modification apportée	Commentaires
Hypothèse	H18.Services_Tiers_De_Confiance	Ajout des éléments	-
Objectif	OE18.Services_Tiers_De_Confiance		Afin de couvrir l'hypothèse H18

8.2.4 La présentation du document

La TOE s'adresse en premier lieu à des applications clientes au travers d'une API, pour lesquelles la question de la visualisation est sans objet. Néanmoins, le contenu du document est transmis en même temps que le résultat de la vérification afin que l'application cliente puisse présenter ce dernier à son propre utilisateur (humain).

Par ailleurs, il est possible, dans les politiques de confiance, d'archiver le document signé, ce qui offre la possibilité, pour un gestionnaire (auditeur) de la TOE, d'accéder au contenu des documents vérifiés et, potentiellement, de les visualiser.

8.2.4.1 Rappel sur les formats

Il importe de ne pas confondre format de signature et format du document signé (par le signataire).

Le format de signature concerne la façon dont la signature à vérifier est transmise à la TOE (section 3.1.3). Il s'agit des formats XML-DSig, XAdES, PKCS #7, CMS et PDF (ce dernier n'est autre qu'une signature CMS d'un document PDF). Ce sont des formats de signature.

Le format du document signé concerne le format du document signé inclus dans la signature à vérifier. Il s'agit des formats « texte brut », HTML et « autres » (PDF, document binaire, etc.). À l'exception d'une signature PDF, qui ne peut concerner qu'un document au format PDF, tous les autres types de formats de signature n'ont pas de restriction sur le format du document signé : celui-ci est une suite d'octets arbitraires inclus sous une forme ou sous une autre dans la signature.

8.2.4.2 Mise en œuvre de la visualisation

La TOE supporte les tous les types de formats pour un document signé mais ne supporte que la visualisation des documents au format « texte brut » ou HTML. Pour ces formats, la visualisation s'appuie sur des applications « standards » (navigateur ou extension du navigateur) identifiées dans les guides d'utilisation. *L'activation de la visualisation coïncide avec les politiques de confiance qui requièrent la conservation des preuves (avec archivage du document signé) et la validation sémantique des documents signés*. En effet, lorsque le document est stable selon les critères de la TOE, il y a l'assurance que ces applications présentent le document signé sans introduire d'ambiguïté sur leur contenu.

Autrement dit, l'activation de la visualisation, pour un format donné, correspond au choix, dans une politique de confiance, de conserver les documents signés dans les preuves archivées et d'imposer la validation sémantique de ces documents ; réciproquement, le choix de ne pas

valider un format document ou de ne pas conserver les documents signés signifie que l'on désactive toute visualisation des documents à ce format.

Par ailleurs, un navigateur pouvant tout aussi reproduire fidèlement un document au format HTML que du « texte brut », la TOE ne considère que les navigateurs comme applications de visualisation potentielles.

Par construction, un gestionnaire utilise un navigateur (qui peut être de référence) pour se connecter à la TOE et consulter les documents validés. En pratique, la visualisation du document signé passe donc par le navigateur de l'opérateur, à charge à celui-ci d'afficher les données qu'il reçoit.

La TOE présente à l'opérateur (gestionnaire ou super-gestionnaire) un bouton permettant d'afficher dans le navigateur courant le document signé et décodé, si la configuration le permet. Dans tous les cas, on présente préalablement à l'opérateur un message lui rappelant quelles sont les applications de référence pour le type de document considéré.

8.2.4.3 Correspondance format-applications

Concernant la capacité donnée à un administrateur de la TOE de configurer les applications en fonction du format (voir « P15.Administration »), la TOE (interface de d'administration) propose une liste d'applications de référence pouvant être associées à une politique de confiance. Cette liste est elle-même définie par le super-administrateur, au même titre que les autres ressources utilisées par la TOE). L'administrateur choisit, parmi cette liste, les applications qu'il tolère pour visualiser les documents.

8.2.4.4 Modifications apportées au profil

Les modifications suivantes ont donc été effectuées :

- Il est supposé que l'application cliente peut afficher le document pour l'utilisateur final
- Une note d'application pour le bien « B.Correspondance_FormatDoc_Application » (p. 31) a été ajoutée, précisant que ce bien correspond à la liste des applications de référence gérée par les super-administrateurs et les administrateurs.
- L'OSP « P7.Possibilité_Présenter_Document » a été modifiée pour demander que la correspondance entre formats de documents et applications de visualisation soit gérée par les administrateurs au niveau organisationnel.
- L'objectif sur l'environnement « OE5.Présentation_Document » a été mis à jour pour prendre en compte la modification de l'OSP « P7.Possibilité_Présenter_Document ».

Catégorie	Nom de l'élément	Modification apportée	Commentaires
Hypothèse	H8.Présentation_Document	Précision	Une note d'application précise le contexte
OSP	P7.Possibilité_Présenter_Document	Précisions, extension	La note présente dans l'OSP précise le contexte et l'OSP.
OSP	P15.Administration	Précision	Une note d'application précise la gestion des différents éléments.
Objectif	O15.Lancement_Applications_Présentation	Précision	Une note d'application précise le contexte
Objectif	O3.Administration	Précision	.Une note d'application a été ajoutée.
Objectif	OE5.Présentation_Document	Extension	Objectif étendu pour conformément à l'extension de l'OSP P7.

Exigence fonctionnelle	FDP_IFF.1/Electronic signature	Précision	- Une note d'application a été ajoutée.

- De plus, le contenu du document est renvoyé à l'application cliente en même temps que le résultat de la validation.

Catégorie	Nom de l'élément	Modification apportée	Commentaires
OSP	P11.Export_Contenu	Ajout des éléments	-
Objectif	O17.Export_Contenu		Afin de couvrir l'OSP P11
Exigence fonctionnelle	FDP_ETC.2/Verification status		-

8.2.5 Le contrôle de sémantique

Le contrôle de sémantique est effectué par la TOE au travers d'un module de contrôle de sémantique.

Dans un premier temps, tout ce qui concerne un module externe de contrôle a donc été supprimé :

Catégorie	Nom de l'élément	Modification apportée	Commentaires
Hypothèse	H.Contrôle_Invariance_Sémantique_Document	Suppression des éléments	-
Objectif	OE.Contrôle_Sémantique_Document_Signé		-

Puis, les composants demandant à la TOE l'utilisation d'un module externe ont été modifiés afin de faire apparaître que le module est *interne*. Le module interne peut retourner trois valeurs possibles : « *stable* », « *unstable* » ou « *not checked* ».

Catégorie	Nom de l'élément	Modification apportée	Commentaires
OSP	P8.Sémantique_Document_Invariante	Précision	DVS ne peut dire si un document est instable. Il indique uniquement si le document peut être instable.
Objectif	O20.Invocation_Module_Controle_Invariance	Précision	Le mot « externe » a été remplacé par « interne »
Exigence fonctionnelle	FDP_IFF.1/Document acceptance	Précisions	Rajout de la capacité d'informer l'application cliente lorsque le statut du contrôle est « not checked »
Exigence fonctionnelle	FDP_ITC.1/Document acceptance	Précision	Le mot « external » a été remplacé par « internal »
Exigence fonctionnelle	FMT_SMF.1/Getting document's semantics invariance status		

Exigence fonctionnelle	FDP_IFF.1/Electronic signature		
Exigence fonctionnelle	FDP_ITC.2/Electronic signature		

8.2.6 La TOE s'adresse à une application et non à un utilisateur humain

Du point de vue de la TOE, les requêtes de vérification de signature ou de validation de certificat sont effectuées par une application et non un humain.

Bien que le profil de protection prenne ce cas en compte au travers du terme « vérificateur », ce dernier a été modifié dans la présente cible de sécurité afin d'établir précisément qui fait appel à la TOE. Les tableaux ci-après résument les modifications apportées au profil sur ce point.

Catégorie	Nom de l'élément	Modification apportée	Commentaires
OSP	P6.Communication_Attributs_Signés	Précision	Le mot « vérificateur » a été changé par « application cliente »
OSP	P12.Export_Données_Validation		
Objectif	O16.Communication_Attributs_Signés		
Objectif	O18.Export_Données_Validation		
Exigence fonctionnelle	FDP_IFC.1/Document acceptance	Précision	Le mot « verifier » est par « client application »
Exigence fonctionnelle	FDP_IFF.1/Document acceptance		
Exigence fonctionnelle	FMT_MTD.1/Selection of the applied signature policy		
Exigence fonctionnelle	FMT_SMF.1/Selection of the applied signature policy		
Exigence fonctionnelle	FDP_IFC.1/Electronic signature		
Exigence fonctionnelle	FDP_IFF.1/Electronic signature		
Exigence fonctionnelle	FDP_ITC.2/Electronic signature		
Exigence fonctionnelle	FDP_IFC.1/Time reference		
Exigence fonctionnelle	FDP_IFF.1/Time reference		
Exigence fonctionnelle	FDP_IFC.1/Certification path		
Exigence fonctionnelle	FDP_IFF.1/Certification path		
Exigence fonctionnelle	FDP_IFC.1/Electronic signature validation		
Exigence fonctionnelle	FDP_IFF.1/Electronic signature validation		
Exigence fonctionnelle	FMT_SMR.1		

Un seul cas fait exception : le mot « vérificateur » ne désigne pas l'application cliente mais l'utilisateur final. Il s'agit du cas de la présentation du document par une application externe.

Catégorie	Nom de l'élément	Modification apportée	Commentaires
Hypothèse	H8.Présentation_Document	Précision	Le mot « vérificateur » est remplacé par « utilisateur final »
Objectif	OE5.Présentation_Document		

Enfin, une précision a été apportée dans l'hypothèse concernant la machine hôte : cette dernière n'est pas sous la responsabilité de chaque vérificateur, mais sous celle d'une personne morale ou physique.

Catégorie	Nom de l'élément	Modification apportée	Commentaires
Hypothèse	H1.Machine_Hôte	Précision	Le texte inutile a été rayé
Objectif	OE2.Machine_Hôte		

Concernant l'interaction avec le « vérificateur » [EXT_DCSSI_PP, 2.4.1], le tableau ci-dessous résume les fonctionnalités de l'interface programmatique de la TOE.

Fonctionnalité du PP	Fonctionnalité de la TOE
Sélection du document à vérifier par le vérificateur	L'application appelante soumet elle-même le document et la signature à vérifier.
Sélection d'une politique de signature à appliquer	voir 8.2.1
Communication/présentation des attributs de signature au vérificateur	Ce point n'est pas applicable dans notre cas : dans la mesure où le vérificateur est une application ayant accès au document et à la signature, elle est à même de connaître les attributs de signature, ce qui n'est pas le cas d'un vérificateur humain (qui peut avoir besoin d'une IHM pour prendre connaissance de ces attributs).
Communication du statut d'exécution	L'interface programmatique communique ces informations dans la valeur de retour.
Communication des données de validation au vérificateur	voir

8.2.7 Export du résultat

La TOE est utilisée par des applications clientes et non par un utilisateur humain directement. Le résultat de la validation est donc transmis à l'application cliente qui le retranscrit pour l'utilisateur final, humain.

La TOE doit donc être capable d'exporter le résultat de la vérification à l'application cliente. C'est ce que traduit l'OSP *P13*.

Catégorie	Nom de l'élément	Modification apportée	Commentaires
OSP	P13.Export_Résultat_Validation	Ajout des éléments	-
Objectif	O19.Export_Résultat_Validation		Afin de couvrir l'OSP P13

8.2.8 Validation de certificats

En plus de répondre à une requête de vérification de signature, la TOE répond aux requêtes de validation de certificat. Ceci ne requiert qu'une précision dans les OSP et objectifs, mais nécessite l'ajout de plusieurs exigences fonctionnelles de sécurité :

Catégorie	Nom de l'élément	Modification apportée	Commentaires
OSP	P12.Export_Données_Validation	Précision concernant la validation de certificat	-
Objectif	O18.Export_Données_Validation		
Exigence fonctionnelle	FDP_IFC.1/Certificate validation	Ajout des exigences	Afin de couvrir l'objectif O18
Exigence fonctionnelle	FDP_IFF.1/Certificate validation		
Exigence fonctionnelle	FMT_MSA.3/Certificate validation status		
Exigence fonctionnelle	FMT_MSA.1/Certificate validation status		
Exigence fonctionnelle	FDP_ETC.2/Certificate validation status		

8.2.9 Fonctionnalités des gestionnaires

Le rôle de gestionnaire est associé à certaines fonctionnalités auxquelles seuls les gestionnaires ont accès.

Ainsi le tableau suivant retrace les modifications apportées par rapport au profil de protection et concernant ces fonctionnalités.

Catégorie	Nom de l'élément	Modification apportée	Commentaires
OSP	P16.Gestion	Ajout des éléments	-
Objectif	O4.Gestion		Afin de couvrir l'OSP P16
Exigence fonctionnelle	FMT_MTD.1/Service report review		Afin de couvrir l'objectif O4
Exigence fonctionnelle	FMT_SMF.1/Service report review		
Exigence fonctionnelle	FMT_MTD.1/Transactions review		
Exigence fonctionnelle	FMT_SMF.1/Transactions review		

8.2.10 Configuration de la TOE

8.2.10.1 Administrateurs

Les administrateurs ne configurent pas uniquement les politiques de signature. En effet, ils peuvent :

- Gérer les applications autorisées à effectuer des requêtes au service
- Gérer les administrateurs et gestionnaires de leur groupe

- Gérer la table d'association spécifiant à quelles ressources politiques de confiance peuvent accéder quelles applications clientes.
- Vérifier les données d'audit de son groupe

Ces fonctionnalités ont été ajoutées au sujet *S3.Administrateur_de_sécurité*.

De plus, comme le contrôle de stabilité est effectué par la TOE, les fonctionnalités les concernant et accessibles aux administrateurs ont été supprimées du sujet *S3.Administrateur_de_sécurité*.

8.2.10.2 Super-administrateurs

Les super-administrateurs sont des sujets ajoutés par rapport au profil de protection. Ils peuvent :

- Gérer les administrateurs, les super-administrateurs, les gestionnaires et les super-gestionnaires du service
- Gérer les ressources accessibles aux administrateurs de sécurité (serveur d'horodatage, OCSP, autorité de certification référencées…)
- Vérifier les données d'audit de son groupe

Ce sujet a été ajouté au travers de *S2.Super-Administrateur_de_sécurité*.

Ces modifications ont un impact significatif dans la suite du document, par rapport au profil de protection. Notamment la menace *M1* du profil de protection peut être étendue aux nouvelles fonctionnalités.

De plus, comme la TOE signe le fichier de configuration que lui a transmis l'administrateur, l'objectif de sécurité sur l'environnement***Erreur ! Source du renvoi introuvable.*** OE16.Protection_Clé_Signature_Configuration permet de participer à la couverture de la menace *M1* en demandant que les clés de la TOE soient protégées par un HSM.

Le tableau suivant détaille les changements apportés à la cible de sécurité par rapport au profil de protection.

Catégorie	Nom de l'élément	Modification apportée	Commentaires
Sujet	S2.Super-Administrateur_de_sécurité	Ajout	-
Sujet	S3.Administrateur_de_sécurité	Modifications	-
Menace	M1.Modification_Ens_Politiques_Signature		Il a été ajouté les tentatives de modification de la configuration de la TOE en général. Le titre de la menace n'a cependant pas été changé afin de rester cohérent avec celui du PP.
OSP	P14.Super-Administration	Ajout	-
OSP	P15.Administration	Précisions	-
Objectif	O2.Super-administration	Ajout	Afin de couvrir l'OSP P14
Objectif	O3.Administration	Précisions	Afin de couvrir l'OSP P15
Objectif	O7.Gestion_Configuration	Ajout des objectifs	Afin de couvrir les ajouts dans la menace M1.

Catégorie	Nom de l'élément	Modification apportée	Commentaires
Objectif	O22.Protection_données_de_configuration		Contribue à la couverture de la menace M1
Objectif	OE16.Protection_Clé_Signature_Configuration**Erreur ! Source du renvoi introuvable.**		Afin de participer à la couverture de la menace M1, car la configuration repose sur sa signature par la TOE
Exigence fonctionnelle	FMT_MTD.1/Super-Administrator-Set of authorized users	Ajout des exigences	Afin de couvrir les objectifs O2, O3 et O7
Exigence fonctionnelle	FMT_SMF.1/Super-Administrator-Management of authorized users set		
Exigence fonctionnelle	FMT_MTD.1/Administrator-Set of authorized users		
Exigence fonctionnelle	FMT_SMF.1/Administrator-Management of authorized users set		
Exigence fonctionnelle	FMT_MTD.1/Set of authorized applications		
Exigence fonctionnelle	FMT_SMF.1/Management of authorized applications set		
Exigence fonctionnelle	FMT_MTD.1/Client application/trust policies association table		
Exigence fonctionnelle	FMT_SMF.1/Management of client application/trust policies association table		
Exigence fonctionnelle	FMT_MTD.1/Set of Resources		
Exigence fonctionnelle	FMT_SMF.1/Management of resources set		
Exigence fonctionnelle	FPT_TDI.1/ Configuration data integrity		Afin de couvrir l'objectif O22
Exigence fonctionnelle	FIA_UAU.1/(Super-)Administrator authentication	Modifications	Pour prendre en compte les opérations que peuvent effectuer les administrateurs et super-administrateurs par rapport à celles du PP

Les données de configuration se présentent sous la forme d'un fichier (chargé en mémoire au démarrage de la TOE), c'est pourquoi, l'objectif *O22.Protection_données_de_configuration* a été ajouté pour contribuer à la couverture de la menace *M1*.

8.2.11 L'audit

La TOE audite les opérations qu'effectue un super-administrateur ou un administrateur lorsqu'il modifie la configuration de la TOE. Ceci a été traduit au travers des modifications suivantes.

Catégorie	Nom de l'élément	Modification apportée	Commentaires
OSP	P17.Audit	Ajout des éléments	-
Objectif	O5.Audit		Afin de couvrir P17
Objectif	O23.Protection_pistes_audit		
Exigence fonctionnelle	FAU_GEN.1/Super-administrator actions audit	Ajout des exigences	Afin de couvrir l'objectif O5
Exigence fonctionnelle	FAU_GEN.2/super-administrator actions audit		
Exigence fonctionnelle	FAU_SAR.1/Super-administrator actions audit		
Exigence fonctionnelle	FAU_STG.1/Super-administrator actions audit		
Exigence fonctionnelle	FAU_GEN.1/Administrator actions audit		
Exigence fonctionnelle	FAU_GEN.2/Administrator actions audit		
Exigence fonctionnelle	FAU_SAR.1/Administrator actions audit		
Exigence fonctionnelle	FAU_SAR.2/ Restricted Audit review		
Exigence fonctionnelle	FAU_STG.1/Administrator actions audit		

9. ARGUMENTAIRE

Nota Bene : L'argumentaire complet est disponible dans la cible d'évaluation **[ST]**.

9.1 Argumentaire pour la résistance des fonctions

Le niveau minimum de résistance est SOF-high, car il est requis par le processus de qualification standard **[QUA-STD]**.

9.2 Argumentaire pour l'ajout du composant étendu FDP_MRU.1

L'argumentaire pour l'ajout du composant étendu FDP_MRU.1 se décompose en la définition du composant, d'une part, l'argumentaire proprement dit, d'autre part.

9.2.1 Définition du composant

La définition générique du composant est la suivante :

Family behaviour

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

Component levelling

FDP_MRU Mandatory rules	1

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

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

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

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

Management: FDP_MRU.1

There are no management activities foreseen for these components.

Audit: FDP_MRU.1

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

a) Minimal: The invocation of a rule.

FDP_MRU.1 Mandatory rules

Hierarchical to: No other components.

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

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

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

FMT_MSA.3 Static attribute initialisation

9.2.2 Argumentaire pour l'ajout

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

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

9.2.3 Testabilité du composant

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

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

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

9.2.4 Applicabilité des exigences d'assurance

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

9.3 Argumentaire pour l'ajout du composant étendu FPT_TDI.1

L'argumentaire pour l'ajout du composant étendu FPT_TDI.1 se décompose en la définition du composant, d'une part, l'argumentaire proprement dit, d'autre part.

9.3.1 Définition du composant

Family behaviour

This family defines the requirements for the test of the TSF data integrity. TSF data testing can occur at any time: at start-up, periodically, at the request of the authorised user, or when other conditions are met.

Component levelling

FPT_TDI TSF data integrity testing	1

FPT_TDI.1 TSF data integrity testing is meant to be used to detect modification of TSF data and requires to specify actions to be taken when integrity errors occur.

The PP/ST author may iterate this component to address different parts of the TSF data.

Management: FPT_TDI.1

The following actions could be considered for the management functions in FMT:

a) management of the types of modification against which the TSF should protect;

b) management of the mechanism used to provide the protection of the data in transit between different parts of the TSF;

c) management of the types of modification of TSF data the TSF should try to detect;

d) management of the actions that will be taken.

Audit: FPT_TDI.1

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

a) Minimal: detection of modification of TSF data;

b) Basic: the action taken following detection of an integrity error.

FPT_TDI.1 TSF data integrity testing

Hierarchical to: No other components.

FPT_TD1.1.1 The TSF shall be able [selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions* [assignment: *conditions under which self test should occur*]] to detect [selection: *modification of data, substitution of data, re-ordering of data, deletion of data,* [assignment: *other integrity errors*]] of [selection: [assignment: *parts of the TSF data*], *TSF data*].

FPT_TD1.1.2 Upon detection of a data integrity error, the TSF shall take the following actions: [assignment: *specify the action to be taken*].

Dependencies: No dependencies

9.3.2 Argumentaire pour l'ajout

L'ajout du composant étendu FPT_TDI.1 a été suscité par le fait que la seule détection de modification de données (ou d'une partie des données) de la TSF n'existe pas dans les exigences fonctionnelles de sécurité. L'exigence FPT_ITT.3 traite de l'intégrité des données de la TSF lorsque celles-ci sont transférées entre deux parties de la TOE. Tandis que FPT_TST requiert seulement la possibilité à l'utilisateur de vérifier l'intégrité des données de la TSF, ainsi que le bon fonctionnement d'opérations définies lors de son instanciation et l'intégrité de son code d'exécution.

Le nouveau composant FPT_TDI.1 permet de requérir que la TOE détecte une modification des données (ou partie des données) de la TSF au moment défini dans l'instanciation du composant.

9.3.3 Testabilité du composant

Le composant fonctionnel étendu FPT_TDI.1 s'apparente à FPT_ITT.3 par le fait qu'il requiert la détection d'erreur d'intégrité sur les données (ou partie des données) de la TSF, ne se différenciant de ce dernier que sur le moment où le contrôle d'intégrité doit être fait.

Puisque FPT_TDI.1 est similaire à un composant bien défini dans le catalogue standard des exigences fonctionnelles de sécurité, il en va de même pour ce composant étendu.

Les éléments d'exigences définis dans le composant étendu FPT_TDI.1 sont donc testables et traçables à travers les différentes représentations de la TOE au même titre que dans l'exigence FPT_ITT.3.

9.3.4 Applicabilité des exigences d'assurance

Comme précisé au paragraphe précédent, le composant FPT_TDI.1 s'apparente au composant FPT_ITT.3. Pour cette même raison, les exigences d'assurances sont applicables pour supporter la nouvelle exigence fonctionnelle, au même titre que pour l'exigence FPT_ITT.3.

10. ANNEXE A – CONTRAINTE SUR LE FORMAT HTML

Le détail des contraintes n'est pas disponible dans la version publique de ce document. Les contraintes sont détaillées dans le document **[ST].**

11. ANNEXE B – DEFINITIONS

Autorité de certification qualifiée

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

Certificat électronique

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

Un certificat électronique doit comporter :

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

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

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

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

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

f) Le code d'identité du certificat électronique ;

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

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

Certificat électronique qualifié

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

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

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

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

Condensé ou condensat

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

Cryptographic Service Provider (CSP)

En français, fournisseur de services cryptographiques.

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

Dispositif de création de signature électronique

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

Dispositif sécurisé de création de signature électronique

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

Dispositif de vérification de signature électronique

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

Données de création de signature électronique

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

Données de vérification de signature électronique

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

Format de contenu

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

Object Identifier (OID)

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

Politique de signature

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

Prestataire de services de certification électronique

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

Qualification des prestataires de services de certification électronique

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

Signataire

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

Signature électronique

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

Signature électronique sécurisée

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

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

Signature électronique présumée fiable

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

On parle aussi de signature électronique qualifiée.

Signature numérique

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

Système de création de signature

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

Pour plus d'information, contactez Dictao au (+33) 1 73 00 26 00
mél : **info@dictao.com** ou visitez notre site web **www.dictao.com**.