Architect of an Open World™

Cible de sécurité

MetaSIGN-APPLET

www.bull.com

Statut

Rédaction	Vincent KAHOUL
Validation	Limité entreprise
Classification	Diffusion restreinte
Statut du document	Version de travail
Version actuelle	1.14
Référence	EVALCC-MSIGN-ST-02

Diffusion

Philippe Blot	ANSSI
Aurélien Leteinturier	ANSSI
Certificateurs	ANSSI
Evaluateurs	OPPIDA

Historique des révisions

Date	Version	Commentaire
01/06/2012	0.1	Création à partir de EVALCC-MSIGN-02
23/08/2012	0.2	Prise en compte des commentaires ANSSI
05/09/2012	0.3	Prise en compte des commentaires ANSSI suite à réunion du 05/09/2012
07/09/2012	1.0	Version validée par le bureau qualification de l'ANSSI
10/10/2012	1.1	Prise en compte des remarques du bureau certification de l'ANSSI pour acceptation de la demande de certification
04/03/2013	1.2	Prise en compte des remarques de l'évaluateur (RTI ASE du 07/02/2013)
26/06/2013	1.3	Prise en compte des remarques de l'évaluateur (RTI ASE version 2.0 du 19/04/2013)
19/01/2014	1.4	Prise en compte des remarques de l'évaluateur (RTI ASE version 3.0 du 24/09/2013) Prise en compte des remarques du bureau certification de l'ANSSI
25/04/2014	1.5	Prise en compte des remarques de l'évaluateur (RTI ASE version 4.0 du 14/04/2013)
01/07/2014	1.6	Prise en compte des remarques de l'évaluateur suite à la réunion du 17/06/2014 Mise à jour des versions des normes ETSI supportées par la TOE
08/09/2014	1.7	Prise en compte des remarques de l'évaluateur (RTI ASE version 5.0 du 05/09/2014)
12/09/2014	1.8	Ajout d'un tableau permettant d'identifier les versions des librairies utilisé par la TOE Ajout de précisions sur la plateforme d'évaluation de la TOE
18/09/2014	1.9	Prise en compte des remarques de l'évaluateur (RTI ASE version 6.0 du 18/09/2014)
30/09/2014	1.10	Prise en compte des remarques de l'évaluateur (RTI ASE version 7.0 du

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

		23/09/2014) Ajout de précisions sur l'identification du SCDev Retrait des références à la taille de clé RSA 1024 bits et 4096 bits Version de la TOE changée à 3.3.1 Prise en compte des remarques de l'évaluateur (RTI ADV_TDS version 2.0 du 26/03/2015) Modification de la référence du SCDev utilisé dans l'environnement d'évaluation de la TOE Précision sur l'arrêt du processus de signature dès qu'une erreur se produit et sur l'arrêt du processus de vérification dès que l'état de la signature est considéré comme invalide Ajout d'une note d'application indiquant que les politiques de signature ne permettent pas de requérir un certificat « qualifié » Modification de F.Présentation_Attributs : les attributs de signature sont affichés uniquement lors du processus de signature. Ajout d'une note d'application dans FMT_MSA.1/Signature attributes afin de définir la liste des attributs de signature. Ajout d'une note d'application dans FDP.IFF 1.2/Time Reference rappelant que le service d'horodatage est supposé de confiance.
27/07/2015	1.11	Mise à jour en accord avec la version 3.3.3 de MetaSIGN-APPLEt Ajout d'une note d'application dans FDP_IFF.1.2/Electronic signature indiquant que le viewer est toujours activé
06/10/2015	1.12	Modification de la version de la TOE (3.3.4) Mise à jour des versions des librairies composant la TOE
27/10/2015	1.13	Mise à jour des librairies composant la TOE
30/11/2015	1.14	Modification de la version de la TOE (3.3.5)

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

Contents

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

1 Introduction

1.1 Identification de la cible de sécurité (ST)

Titre de la ST	Bull MetaSIGN-APPLET – Security Target
Référence de la ST	EVALCC-MSIGN-ST-02/v1.14
Identifiant de la TOE	MetaSIGN-APPLET v3.3.5
Conformité aux CC	Common Criteria for Information Technology Security Evaluation, Version 3.1 R3
Conformité à un PP	La cible de sécurité est conforme aux profils de protection : - « Application de création de signature électronique » [PP-ACSE-CCv3.1], version 1.7 du 2 mars 2011 - « Module de vérification de signature électronique » [PP-MVSE-CCv3.1], version 1.7 du 2 mars 2011
Niveau d'assurance	Le niveau d'assurance visé est le niveau EAL3 augmenté des composants d'assurance AVA_VAN.3 et ALC_FLR.3. Conformément au processus d'évaluation de niveau « Qualification Standard » de l'ANSSI.

1.2 Identification de la cible d'évaluation (TOE)

Développeur	Bull
Nom du produit	MetaSIGN-APPLET
Version	V3.3.5
Plateforme cible	Voir 1.4.2

1.3 Vue d'ensemble de la cible d'évaluation

Dans le cadre de la dématérialisation des procédures et des échanges, les organisations souhaitent de plus en plus disposer d'applications supportant la signature électronique et notamment la signature électronique avancée (appelée "signature électronique sécurisée" dans le Décret no 2001-272 du 30 mars 2001 modifié par le Décret no 2002-535 du 18 avril 2002).

MetaSIGN constitue l'offre de signature électronique avancée de Bull. Cette offre est tout d'abord disponible sous la forme d'une interface programmatique en langage Java qui a pour but de faciliter l'intégration de la signature électronique dans les applications. . Cette interface programmatique est dénommée MetaSIGN-API.

MetaSIGN-APPLET, qui s'appuie sur MetaSIGN-API, permet d'offrir des services de signature et de vérification de signature équivalents dans les navigateurs Internet pour être au plus proche de l'utilisateur.

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

La cible d'évaluation (ou TOE – Target Of Evaluation) est MetaSIGN-APPLET.

1.4 Description de la cible d'évaluation

La cible d'évaluation (ou TOE – Target Of Evaluation) est un ensemble d'applets de MetaSIGN, dénommée MetaSIGN-APPLET dans la suite du document, et permettant la création et la vérification de signatures électroniques aux formats suivants :

- CAdES : CMS Advanced Electronic Signature, défini dans la spécification technique ETSI TS 101 733 (version 2.2.1) (2013-04) ;
- XAdES : XML Advanced Electronic Signature, défini dans la spécification technique ETSI TS 101 903 (version 1.4.2) (2010-12) ;
- PAdES : PDF Advanced Electronic Signature, défini dans la spécification technique ETSI TS 102 778-2 (version 1.2.1) (2009-07), TS 102 778-3 (version 1.2.1) (2010-07) et TS 102 778-4 (version 1.1.2) (2009-12)
- CMS (RFC 3852) : Format de signature numérique basique (hors périmètre d'évaluation de la TOE car ne constitue pas une signature électronique avancée)

MetaSIGN-APPLET utilise un dispositif de création de signature électronique, hors périmètre d'évaluation. Ce dispositif est le seul à posséder la clé privée du signataire et à pouvoir l'utiliser. Ce dispositif peut être :

- Une carte à puce (cartes à puce certifiées Critères Communs et/ou qualifiées, à travers l'interface normalisée PKCS #11) ;
- Un token USB (à travers l'interface normalisée PKCS #11) ;
- Un HSM (à travers l'interface normalisée PKCS #11) ;
- Un fichier protégé (au format normalisé PKCS #12).

MetaSIGN-APPLET supporte la signature (et la vérification de signature) de documents aux formats suivants :

- XML ;
- Texte brut ;
- PDF ;
- Microsoft Office ;
- Open Office.
- Tout autre format (flux de données binaires)

Pour réaliser les différentes opérations de signature et de vérification de signature, ainsi que l'utilisation du dispositif de création de signature, MetaSIGN-APPLET s'appuie sur MetaSIGN-API.

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

Cette librairie fait l'objet d'une évaluation Critères Communs. Ainsi, MetaSIGN-API est une libraire qui compose la TOE.

Suivant le format du document à signer ou à vérifier, MetaSIGN-APPLET permet de lancer l'application de visualisation adéquate, en se basant sur sa configuration (table de correspondance entre un format de document et une application de visualisation externe). Les applications de visualisation externes sont hors du périmètre d'évaluation. Toutefois, MetaSIGN-APPLET intègre nativement un mécanisme de visualisation pour les fichiers de type texte brut (extension « txt »).

Dans un usage courant, la TOE est intégrée dans une application « métier » permettant de doter celles-ci des fonctions de création et/ou de vérification de signatures électroniques. La TOE est donc exécutée suite à son appel par l'application « métier » (nommée par la suite application utilisatrice).

MetaSIGN-APPLET fonctionne toujours en local sur sa machine appelante (poste de travail ou serveur). Les ressources nécessaires (le fichier de configuration, les politiques de signature) doivent être disponibles sur cette même machine ou sur une machine distante. Les ressources cryptographiques doivent être disponibles sur la machine local.

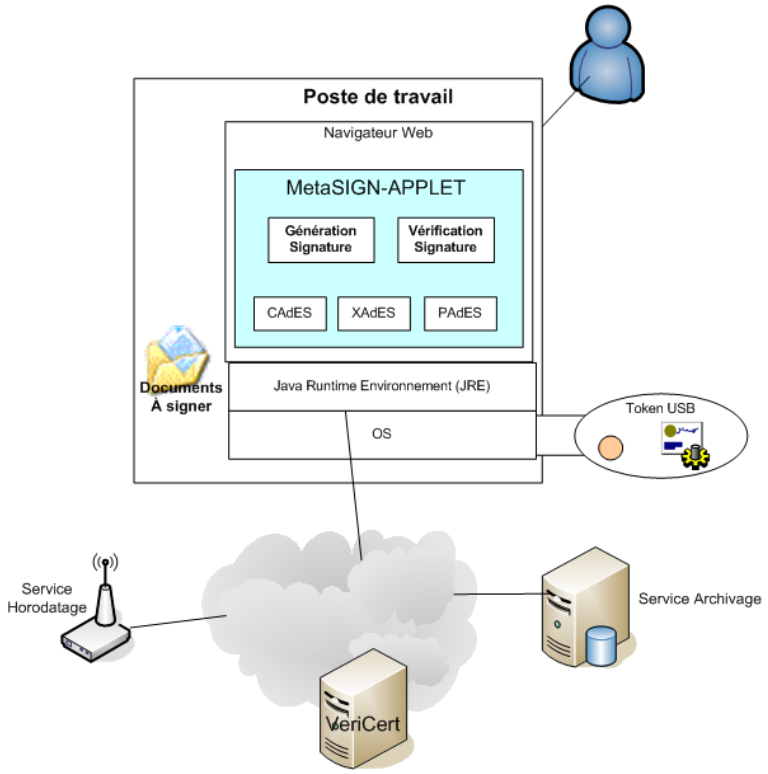
Le document à signer ou à vérifier est fourni à la TOE en tant que paramètre par l'application utilisatrice, avec éventuellement la politique de signature à utiliser (politique explicite), et d'autres paramètres présentés ci-après.

MetaSIGN-APPLET peut donc être utilisée pour développer une application Web de création de signature et/ou de vérification de signature sur le poste utilisateur.

Le schéma suivant illustre à titre d'exemple des utilisations possibles de MetaSIGN-APPLET, pour doter des applications « poste de travail » avec des fonctions de création ou vérification de signatures :

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS



1.4.1 Description des services fournis par la TOE

1.4.1.1 Description des services

MetaSIGN-APPLET est un ensemble d'applets et interfaces graphique permettant la mise en œuvre de la signature avancée dans les applications Web appelantes au travers des services suivants :

- L'applet de génération d'une signature électronique avancée, d'un document ou d'un flot de données, en utilisant un dispositif sécurisé de création de signature électronique (module cryptographique hors périmètre d'évaluation) ;
- L'applet de vérification d'une signature électronique avec, optionnellement, l'augmentation de la signature. L'augmentation consiste à collecter les données de vérification (certificats d'AC, CRLs, horodatage,…) qui seront utilisées lors de la vérification ultérieure ; Dans le cas d'une vérification d'une signature avec augmentation de celle-ci, une nouvelle signature est alors renvoyée et contient les données de vérification demandées. Un rapport de vérification est émis.

Chacune de ces applets peut être utilisée de manière indépendante, par une application utilisant MetaSIGN-APPLET.

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

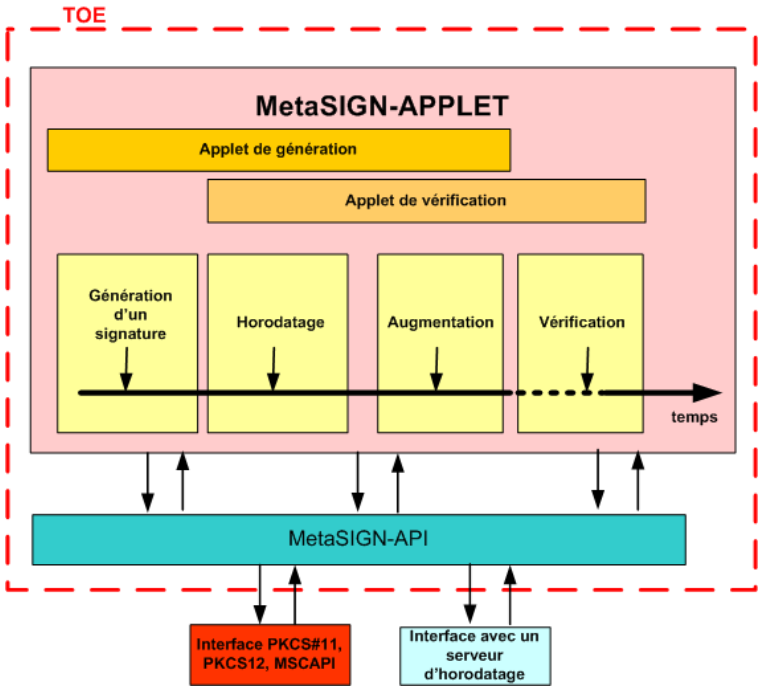
MetaSIGN-APPLET supporte les formats de signature suivants pour la création et la vérification de signature ainsi que pour le cachet :

- CAdES (ETSI TS 101 733) : formats CAdES-BES, CAdES-EPES, CAdES-T, CAdES-C, CAdES-X-L et CAdES-A ;
- XAdES (ETSI TS 101 903) : formats XAdES-BES, XAdES-EPES, XAdES-T, XAdES-C, XAdES-X-L et XAdES-A ;
- PAdES (ETSI TS 102 778) : format CMS (Part 2), PAdES-BES (Part 3), PAdES-EPES (Part 3) PAdES-T (Part 3) et PAdES-LTV (Part 4).
- CMS (RFC 3852) : Format de signature numérique basique (hors périmètre d'évaluation de la TOE car ne constitue pas une signature électronique avancée)

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

Le schéma suivant présente les différentes opérations invoquées lors de la constitution, et lors de vérification de signature, en utilisant les services de MetaSIGN-APPLET. Ces opérations sont ordonnées temporellement :



Fonctionnalités de MetaSIGN-APPLET

1.4.1.2 Description du contenu des politiques de signature utilisée par MetaSIGN-APPLET

Une politique de signature est utilisée pour la génération et pour la vérification d'une signature avancée. Le format de description de cette politique de signature utilisée par MetaSIGN-APPLET est conforme au format XML des politiques de signature défini par [TR 102 038] avec quelques restrictions sur les champs optionnels :

- L'application de règles sur différents types d'engagements : les règles ne sont appliquées que sur une seule liste de types d'engagement
- Le champ (optionnel) d'application du type d'engagement n'est pas supporté ;
- Seules les propriétés signées obligatoires sont supportées ;
- Le champ (optionnel) sur les contraintes de politiques associées à la chaîne de confiance défini dans la politique n'est pas supporté ;
- Le champ (optionnel) sur les contraintes sur les des autorités d'horodatage n'est pas supporté ;

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

- Le champ (optionnel) sur les contraintes des attributs des certificats du signataire et de la chaîne de confiance.

La politique de signature est un ensemble de règles pour la création et la vérification d'une signature électronique, sous lesquelles une signature électronique peut être déterminée comme valide. Une politique de signature est référencée par un OID (Object Identifier) qui a pour but de référencer unitairement la politique, sans équivoque possible.

Les paramètres supportés par la politique de signature de MetaSIGN sont les suivants :

- Le nom et la description textuelle de la politique de signature ;
- L'identifiant unique (OID) de la politique de signature ;
- L'identifiant des fonctions de hachage utilisables ;
- Les certificats des AC Racines de confiances autorisées pour le certificat du signataire ;
- Les valeurs autorisées de l'extension « certificatePolicies » du certificat du signataire et de la racine ;
- Tests de la révocation du certificat du signataire et de la validité des CRLs ;
- Les valeurs autorisées de l'extension « keyUsage » du certificat du signataire : présence des bits digital signature et non répudiation ;
- Période de grâce pour le certificat du signataire ;
- Les types d'engagements acceptés ;
- Les certificats des AC Racines de confiances autorisées pour le certificat de l'autorité d'horodatage ;
- Les valeurs autorisées de l'extension « certificatePolicies » du certificat de l'autorité d'horodatage ;
- Tests de la révocation du certificat de l'autorité d'horodatage et de la validité des CRLs ;
- Période de grâce pour le certificat de l'autorité d'horodatage.

Les politiques de signatures sont localisées dans un magasin de politiques, géré par l'administrateur (assuré par l'application utilisatrice) de la TOE.

L'application appelante fournit la localisation du magasin des politiques de signatures lors d'un appel au module de configuration d'une applet de MetaSIGN-APPLET.

L'application appelante fournit l'identifiant de la politique de signature à utiliser pour une opération de signature ou de vérification lors d'un autre appel au module de configuration d'une applet de MetaSIGN-APPLET.

1.4.2 Architecture de la TOE

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

1.4.2.1 Architecture physique

MetaSIGN-APPLET est un ensemble d'applets et d'interfaces graphiques permettant une intégration simplifiée de la signature électronique dans les applications Web. Elle est livrée avec sa documentation complète et exhaustive, sous la forme d'une application Java (fichiers .jar signes), permettant de vérifier l'authenticité et l'intégrité des applications avant de les utiliser (l'outil de signature des fichiers jar et de vérification est hors du périmètre d'évaluation).

Cette application est utilisée par des développeurs qui dotent les applications clientes des fonctions de création et/ou de vérification de signatures en utilisant ces applets.

L'utilisation de MetaSIGN-APPLET requière la présence d'un environnement d'exécution Java JRE Sun/Oracle 6 update 31 ou supérieur sur le poste de travail sur lequel est installé et exécuté MetaSIGN-APPLET.

La liste des fichiers java de MetaSIGN-APPLET est composée de 3 types de fichiers :

- L'application Java MetaSIGN-APPLET : metasign-applet.jar ;
- Les librairies externes développées par Bull :
  - metasign-api.jar : la librairie MetaSIGN-API ;
  - common.jar : utilitaires pour la gestion de fichiers, des magasins...
  - com.bull.security.common.server.connection.jar : pour la gestion des connexions sécurisée aux serveurs distants ;
  - com.bull.security.common.checker.certificate.jar et com.bull.security.common.checker.jar : pour le contrôle de validité des certificats ;
  - com.bull.security.common.semantics.jar : pour le contrôle de l'invariance sémanatique (non applicable à MetaSIGN-API)
  - com.bull.security.viewer.jar : pour la gestion de la visualisation des documents (non applicable à MetaSIGN-API)
  - hsm_tools.jar : pour la communication avec un module cryptographique (HSM et carte à puce)
  - com.bull.security.utils.net.jar : permet la gestion des types MIME sur les fichiers.
  - forms.jar : permet la gestion des formulaires
  - com.bull.security.common.jaxb.adapters.jar : adapteurs JAXB
- Les librairies externes
  - iaik_cms.jar : gère la syntaxe cryptographique ASN1 ;
  - iaik_tsp.jar : fournit les fonctionnalités pour développer un client d'horodatage ;
  - iaikPkcs11Wrapper.jar, iaikPkcs11Provider.jar : permet d'interfacer les modules PKCS#11 ;
  - iaik_jce_full.jar : implémentation des fonctions cryptographiques ;

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

- iaik_xades.jar, iaik_xsect.jar : permettent le traitement et la manipulation des signatures XAdES et XMLDSig ;
- iaik_ssl.jar, w3c_http.jar : pour la gestion des connexions sécurisées aux serveurs distants ;
- iaik_hlapi.jar : pour la vérification et la construction des chaînes de certification et la gestion de clés et de certificats ;
- iaik_eccelerate.jar, iaik_eccelerate_addon.jar, iaik_eccelerate_cms.jar, iaik_eccelerate_ssl.jar : pour l'implémentation des algorithmes de courbes elliptiques.
- serializer.jar, xalan.jar, xml-apis.jar : permettent le traitement et la manipulation de de documents XML
- pdfbox.jar : permet la manipulation de documents PDF
- fontbox-1.8.5.jar : utilitaires utilisés par pdfbox ;
- commons-codec.jar : permet le décodage et l'encodage d'objets ;
- commons-httpclient.jar : permet d'établir des connections http ;
- commons-io.jar : utilitaires pour la gestion de fichiers ;
- commons-logging.jar, log4j.jar, slf4j-api-1.6.1.jar, slf4j-log4j12-1.6.1.jar : utilitaires pour la gestion des traces (logs) ;
- jsobject.jar : pour la manipulation d'objets en javascript ;
- forms-1.3.0.jar : gestion de l'interface graphique pour ServerConnection.

Les versions des librairies java de la TOE sont les suivantes :

Nom de la librairie	Fournisseur	Version
metasign-api.jar	Bull SAS	3.3.5
metasign-applet.jar	Bull SAS	3.3.5
iaik_jce_full.jar	IAIK	5.24
iaik_ssl.jar	IAIK	5.0
w3c_http.jar	IAIK	5.0
iaik_xades.jar	IAIK	1.4.2_1.191
iaik_xsect.jar	IAIK	1.191
iaik_cms.jar	IAIK	5.0
iaik_tsp.jar	IAIK	2.31
aikPkcs11Provider.jar	IAIK	1.4
iaikPkcs11Wrapper.jar	IAIK	1.3
iaik_eccelerate.jar	IAIK	2.51
iaik_eccelerate_addon.jar	IAIK	2.51
iaik_eccelerate_cms.jar	IAIK	2.5

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

iaik_eccelerate_ssl.jar	IAIK	2.5
iaik_hlapi.jar	IAIK	1.1
xalan.jar	Apache Software Foundation	2.7.1
xml-apis.jar	Apache Software Foundation	1.3.04
serializer.jar	Apache Software Foundation	2.7.1
common-io.jar	Apache Software Foundation	1.1
forms-1.3.0.jar	Apache Software Foundation	1.3.0
log4j.jar	Apache Software Foundation	1.2.14
slf4j-api-1.6.1.jar	Apache Software Foundation	1.6.1
slf4j-log4j-1.6.1.jar	Apache Software Foundation	1.6.1
jsobject.jar	Apache Software Foundation	NA
pdfbox.jar	Apache PDFBox	1.8.7.SNAPSHOT
fontbox-1.8.5.jar	Apache PDFBox	1.8.5
com.bull.security.common.server.connection.jar	Bull SAS	common_1_37_1
com.bull.security.common.checker.certificate.jar	Bull SAS	common_1_37_1
com.bull.security.common.checker.jar	Bull SAS	common_1_37_1
hsm_tools.jar	Bull SAS	common_1_37_1
com.bull.security.utils.net.jar	Bull SAS	common_1_37_1
com.bull.security.viewer.jar	Bull SAS	common_1_37_1
com.bull.security.common.semantics.jar	Bull SAS	common_1_37_1
common.jar	Bull SAS	common_1_37_1
forms.jar	Bull SAS	common_1_37_1
com.bull.security.common.jaxb.adapters.jar	Bull SAS	common_1_37_1

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

1.4.2.2 Architecture fonctionnelle

L'interface externe de MetaSIGN-APPLET offre les 2 groupes de fonctionnalités suivantes : génération et vérification avec la possibilité d'augmenter la signature. Ces fonctionnalités sont mises en œuvre par les applets suivants :

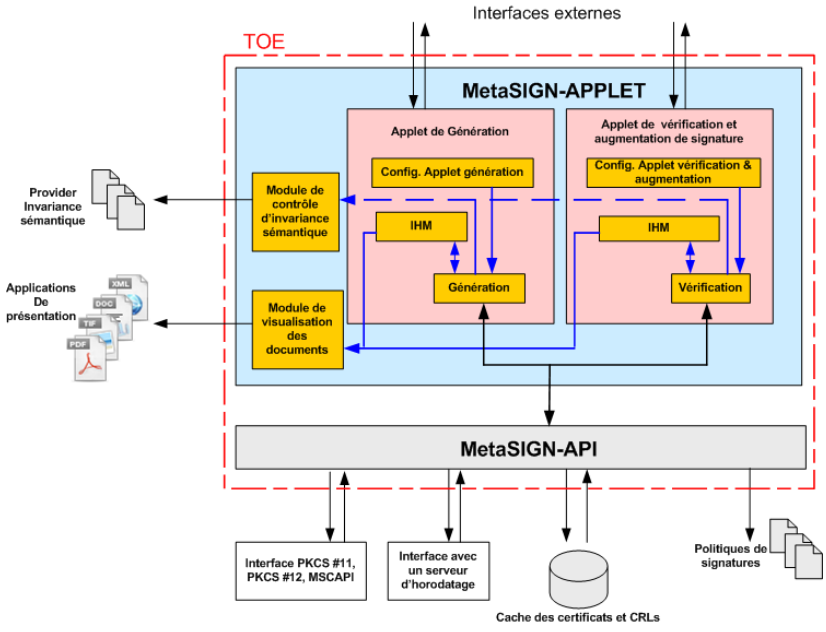
- **Applet de génération d'une signature électronique avancée d'un document ou de données** ;
- **Applet de vérification et d'augmentation d'une signature**.

Chaque applet embarque :

- Un module de configuration : permettant d'initialiser le contexte d'utilisation de l'applet et d'accéder aux modules externes à l'applet (MetaSIGN-API, contrôle d'invariance sémantique, visualisatuer de document) ;
- Un module d'IHM : interface graphique pour l'utilisateur de l'applet ;
- Un module réalisant l'opération offerte par l'applet et en liaison avec MetaSIGN-API.

De plus, MetaSIGN-APPLET s'appuie sur l'utilisation de la librairie MetaSIGN-API qui constitue un module fonctionnel permettant la réalisation des opérations de signatures et de vérification ainsi que la communication avec les interfaces externes (interface avec le dispositif de création de signatures, service d'horodatage, service de validation des certificats, politiques de signatures)

La figure suivante présente une vue schématique de l'architecture fonctionnelle de la cible d'évaluation (TOE). Les modules qui composent la TOE sont décrits dans les chapitres suivants et délimité par les pointillés rouges du schéma ci-dessous :



This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

Les applets peuvent être utilisés indépendamment les uns des autres. Néanmoins les modules de contrôle d'invariance sémantique et de visualisation ainsi que MetaSIGN-API sont utilisés conjointement avec chacun des deux principaux modules (Applet de génération, Applet de vérification).

Applet de Génération de signature

Cette applet permet de générer une signature électronique avancée d'un document ou de données suivant un des formats de signature supportés (CAdES-BES, CAdES-EPES, XAdES-BES, XAdES-EPES, PAdES-BES, PAdES-EPES).

La génération d'une signature électronique sécurisée consiste à signer avec la clé privée du signataire l'empreinte des éléments suivants :

- Le **document à signer** proprement dit ;
- Un **ensemble particulier de propriétés** dénommées propriétés signées (signed properties).

C'est la composition de cet ensemble de propriétés qui fait de la signature générée une signature électronique sécurisée de base.

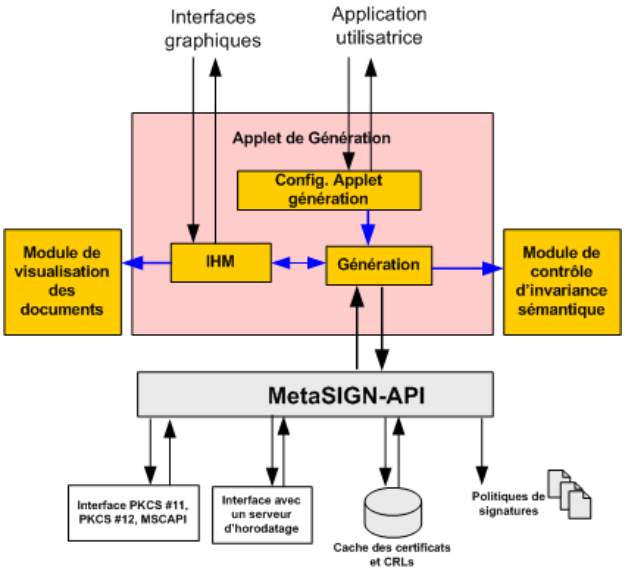
L'applet de génération permet d'augmenter la signature de toutes les valeurs nécessaires à la vérification ultérieure (certificats d'AC, CRLs). Cette opération s'appelle l'augmentation et s'effectue par rapport à une politique de signature déterminée. On obtient alors une signature au format ES-T (ajout d'un jeton d'horodatage), ES-C (signature augmentée par les références) ou, ES-X Long ou LTV (signature augmentée par les valeurs). ES faisant référence aux trois formats CAd**ES**, XAd**ES** et PAd**ES**.

L'applet de génération de signatures permet de générer différents types de signature suivant le format de signature choisie :

- Pour CAdES : Signature enveloppante, Signature détachée ;
- Pour XAdES : Signature enveloppante, Signature enveloppée, Signature détachée ;
- Pour PAdES : Signature enveloppée ;
- Pour CMS : signature enveloppante, Signature détachée (hors périmètre d'évaluation de la TOE).

L'architecture pour l'applet de génération des signatures électroniques est la suivante :

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS



L'applet utilise MetaSIGN-API qui gère les clés et les certificats du signataire en local en utilisant soit l'interface PKCS#11, soit un format PKCS#12 ou encore l'interface MSCAPI permettant d'accéder aux certificats stockés dans le magasin du navigateur Internet Explorer (pour un système Windows uniquement) ainsi que les politiques de signature.

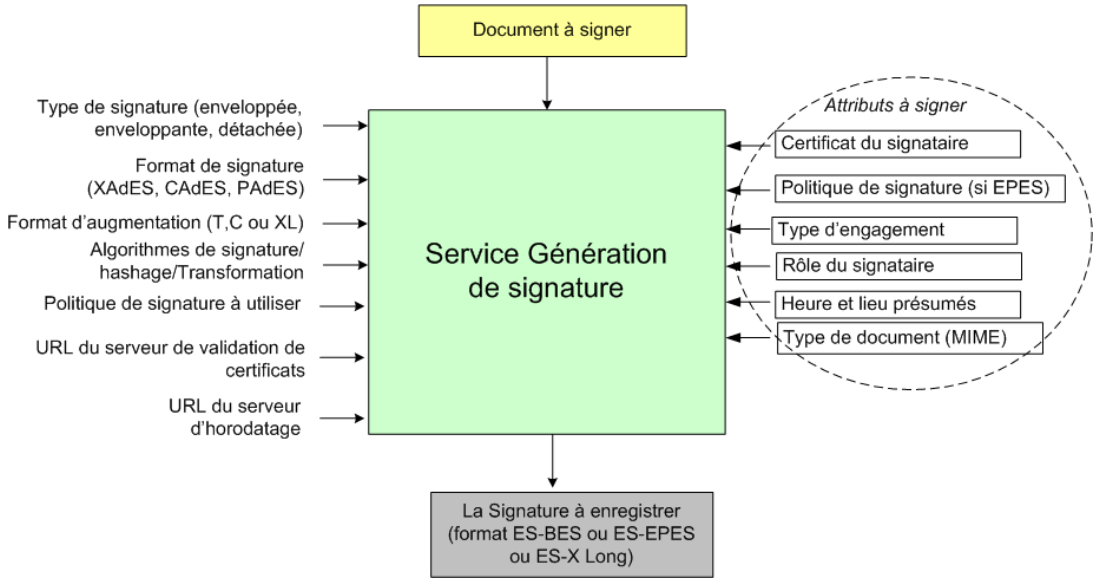
Pour l'horodatage des signatures, l'applet utilise MetaSIGN-API pour faire appel à un serveur d'horodatage dont l'URL doit être paramétrée. Le protocole de communication utilisé est le protocole standard définit dans la RFC 3161 : Time-Stamp Protocol (TSP).

Pour la validation des certificats, l'applet utilise MetaSIGN-API et peut :

- soit utiliser un cache local dans lequel elle conserve les certificats d'AC et les CRL utilisés et ce afin de réduire les appels réseaux
- soit faire appel au serveur de validation de certificats [VeriCert] (hors périmètre d'évaluation de la TOE).

La figure suivante présente les paramètres utilisés en entrée, et ceux produits en sortie de l'applet de génération de signature :

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS



L'applet de génération de signature guide l'utilisateur dans toutes les opérations nécessaires à la génération de la signature. Elle offre une interface graphique, qui lui permet de déclencher l'acte de signer. Cette interface graphique apparait comme une boîte de dialogue dans la page de l'application Web et permet à l'utilisateur de renseigner des paramètres liés à la signature électronique avancée en fonction de la configuration de l'applet.

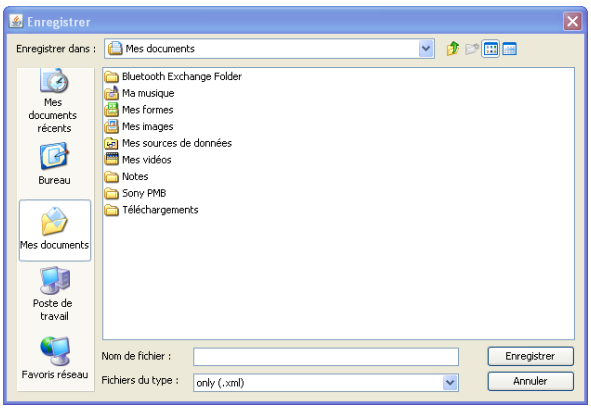
Exemple 1 : Demande simple de signature de document

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

Exemple 2 : Demande de signature de document où le signataire doit préciser 3 paramètres pour la signature

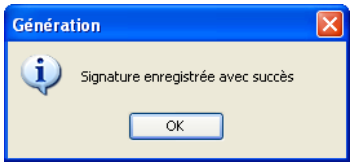
Lorsque la signature a été générée, MetaSIGN-APPLET fournit la signature enveloppée dans le document ou séparée du document (selon de format de signature choisi) :

- En demandant au signataire de définir le répertoire afin qu'elle y soit déposée. Dans ce cas, une fenêtre d'interface graphique est proposée pour déposer la signature :



- en le déposant directement sur le répertoire définit par la configuration de l'applet ou lors de la saisie des paramètres d'entrée.

Une fenêtre s'ouvre alors pour signaler l'enregistrement de la signature avec succès :



This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

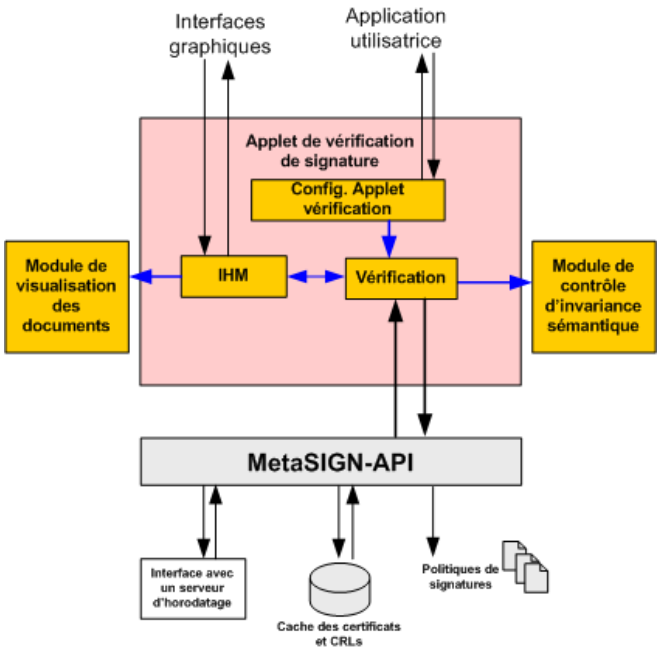
Applet de Vérification et augmentation de signature

La vérification d'une signature électronique consiste à contrôler la signature par rapport à la politique de signature définie. La vérification peut être immédiate avec augmentation de la signature ou ultérieure.

La vérification ultérieure est réalisée en utilisant les éléments qui ont été stockés à l'intérieur de la signature lors de son augmentation. Elle peut être effectuée à tout moment, y compris après la date d'expiration du certificat du signataire.

L'applet de vérification permet aussi de réaliser une vérification immédiate avec augmentation de la signature lorsque cela est demandé, de toutes les valeurs nécessaires à la vérification ultérieure (certificats d'AC, CRLs). Pour ce faire le module de vérification prend en entrée une signature au format ES-BES ou ES-EPES et en sortie, on obtient une signature au format ES-C (signature augmentée par les références) ou ES-X Long (signature augmentée par les valeurs). ES faisant référence aux trois formats CAd**ES**, XAd**ES** et PAd**ES**.

L'architecture pour le module de vérification des signatures électroniques est la suivante :



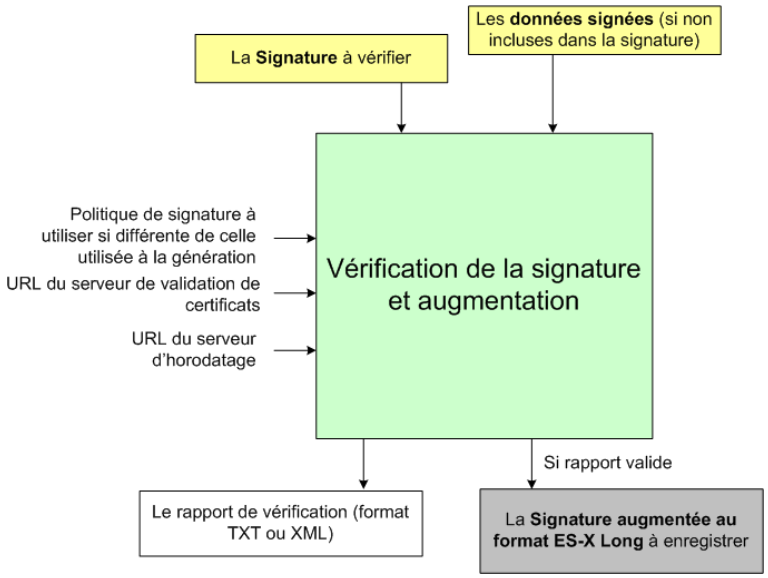
Pour l'horodatage des signatures, l'applet utilise MetaSIGN-API pour faire appel à un serveur d'horodatage dont l'URL doit être paramétrée. Le protocole de communication utilisé est le protocole standard définit dans la RFC 3161 : Time-Stamp Protocol (TSP).

Pour la validation des certificats, l'applet utilise MetaSIGN-API et peut :

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

- soit utiliser un cache local dans lequel elle conserve les certificats d'AC et les CRL utilisés et ce afin de réduire les appels réseaux
- soit faire appel au serveur de validation de certificats [VeriCert] (hors périmètre d'évaluation de la TOE).

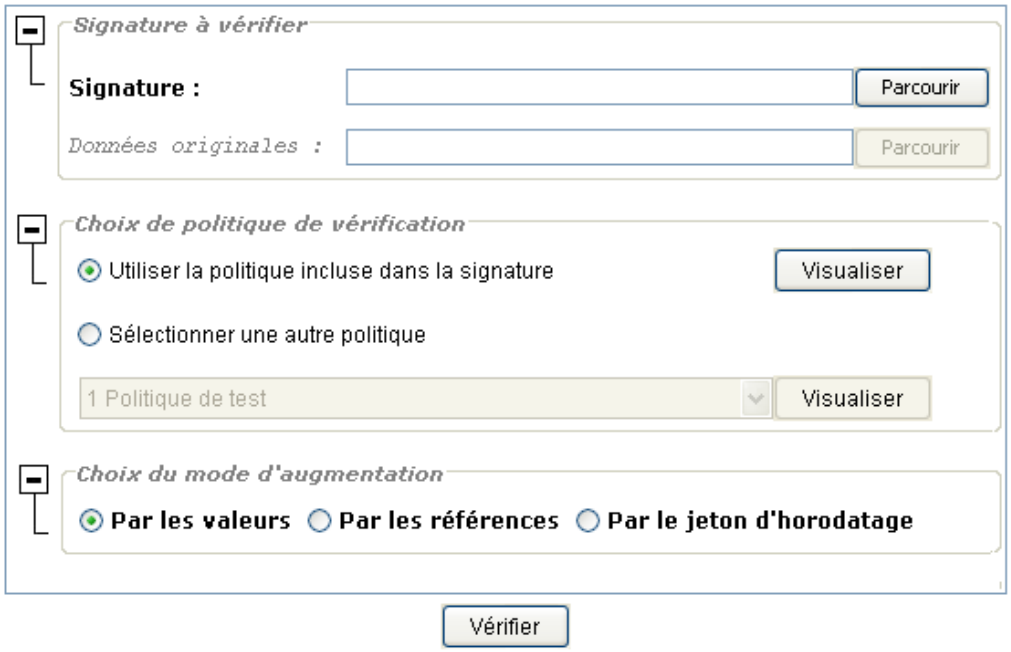
La figure suivante présente les paramètres utilisés en entrée, et ceux produits en sortie du module de vérification immédiate et d'augmentation de signature :



L'applet de vérification de signature guide l'utilisateur dans toutes les opérations nécessaires à la vérification de la signature et permettre ensuite son augmentation et son horodatage. Elle offre une interface graphique, qui lui permet de déclencher l'acte de vérification. Cette interface graphique apparait comme une boîte de dialogue dans la page de l'application Web et permet à l'utilisateur de renseigner des paramètres liés à la signature électronique avancée en fonction de la configuration de l'applet

Copyright 2015 Bull SAS

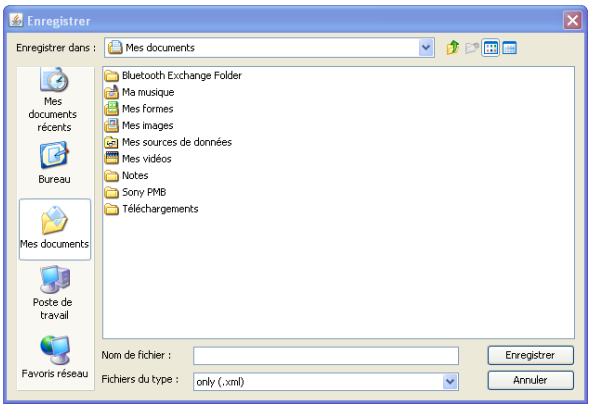
This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS



Exemple 3 : Exemple de demande de vérification immédiate de signature où l'utilisateur doit préciser les propriétés d'objet et de nature de document et un champ optionnel

Lorsqu'une augmentation de la signature a été demandée et générée, MetaSIGN-APPLET fournit la nouvelle signature enveloppée dans le document ou séparée du document (selon de format de signature choisi) :

- En demandant au signataire de définir le répertoire afin qu'elle y soit déposée. Dans ce cas, une fenêtre d'interface graphique est proposée pour déposer la signature :

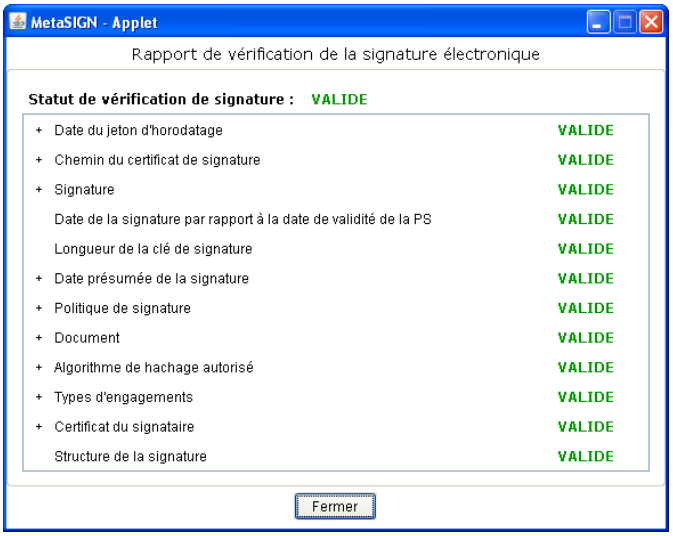


- en le déposant directement sur le répertoire définit par la configuration de l'applet ou lors de la saisie des paramètres d'entrée.

Lorsque la signature a été vérifiée par l'applet, une fenêtre apparaît afin d'en donner l'état de la vérification

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

L'utilisateur a ensuite la possibilité de visualiser le rapport détaillé en sélectionnant « Détails du rapport » si son affichage a été autorisé par la configuration de l'applet :



Module de visualisation de documents

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

La TOE permet, sur demande du signataire ou du vérificateur, le lancement d'une application de présentation correspondant au format du document à visualiser.

Pour ce faire, le module de visualisation de documents de la TOE gère la correspondance entre les formats de document qu'elle accepte et les applications de visualisation. La configuration de l'applet, définie par l'administrateur l'application utilisatrice de la TOE, permet d'établir cette correspondance par un appel à la fonction de configuration du module de visualisation.

Ce module de visualisation implémente en interne la visualisation des documents au format « texte ».

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

Module de contrôle d'invariance sémantique

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

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

D'autre part, le vérificateur qui reçoit ou qui vérifie la signature peut aussi être induit en erreur. Celui-ci pourrait en effet être amené à visualiser un document sémantiquement différent de celui présenté au signataire.
Ainsi, le contenu du document à signer ou à vérifier doit être contrôlé pour attester que sa sémantique ne dépend pas de paramètres qui lui sont extérieurs.

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

Ce module de contrôle d'invariance intègre toutefois un module interne permettant de contrôler les documents au format « texte », considéré alors comme stable.

Le module informe le signataire ou le vérificateur dans le cas où le module externe décèle que la sémantique du document n'est pas stable ou qu'elle ne peut être contrôlée.

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

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

Module de configuration des applets

Chaque applet dispose d'un module de configuration permettant d'initialiser les différents paramètres de configuration qui seront utilisés lors de demandes de signature ou de vérification de signature

Le paramétrage est regroupé en sous-ensembles :

- Les paramètres de définition de l'IHM
- Les paramètres de configuration du module d'invariance sémantique ;
- Les paramètres de configuration du module de visualisation des documents ;
- Les paramètres de configuration de l'utilisation de MetaSIGN-API.

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

1.4.3 Plateforme d'évaluation

MetaSIGN-APPLET est évaluée à travers l'application "type" suivante:

- MetaSIGN-APPLET est chargée dans le navigateur web, utilisant MetaSIGN-API pour créer des signatures électroniques et pour vérifier des signatures électroniques.

Cette application est déployée sur la plateforme hôte décrite ci-après.

1.4.3.1 Plateforme Hôte

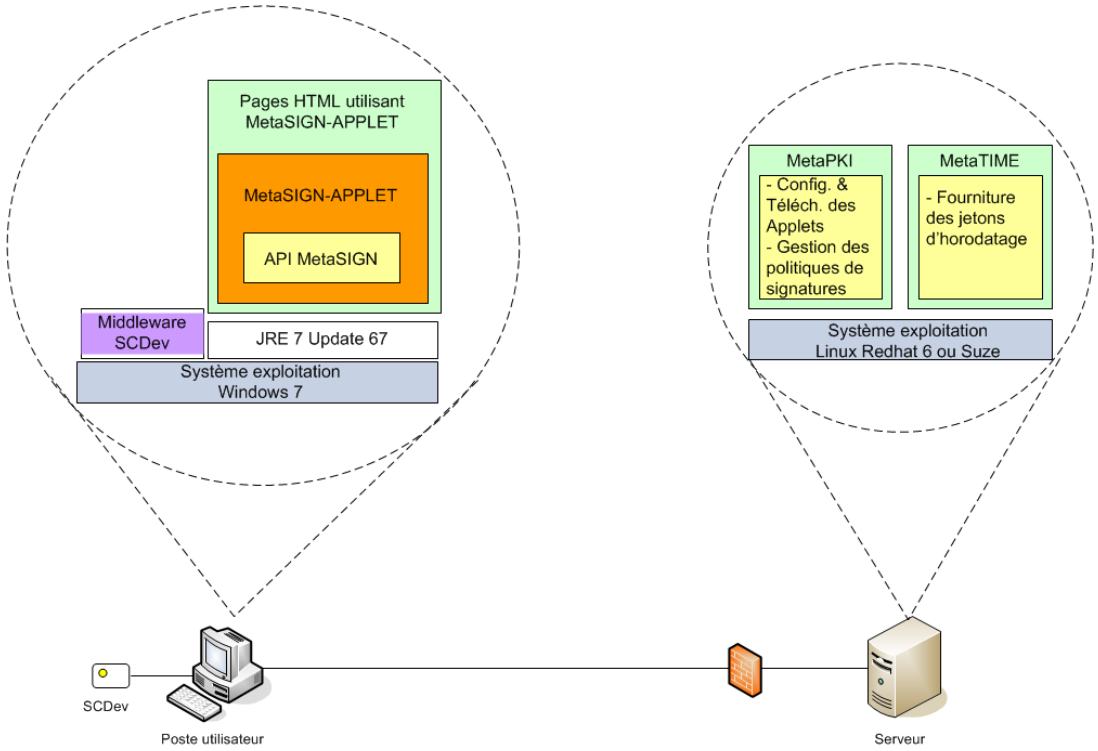
La plateforme est constituée des éléments suivants:

- Ordinateur personnel :
  - Système d'exploitation : Windows 7 ;
  - Les composants logiciels permettant de communiquer avec le dispositif de création de signature (SCDev). Librairie pkcs#11 « IDPrimePKCS11.dll »;
  - Un dispositif de création de signature électronique (SCDev) qualifié au niveau renforcé : carte à puce Gemalto IDPrime MD 840;
  - Le navigateur Internet (Internet Explorer) : version 11 ;
  - L'environnement d'exécution Java : JRE Sun/Oracle 7 update 67
  - Des pages HTML de tests permettant de télécharger les applets de génération et de vérification de signature.
- Un serveur sur lequel est hébergé :
  - Une IGC (Infrastructure de Gestion de clés) permettant de délivrer des certificats de signature de test. Cette IGC est représentée par une instance de MetaPKI (produit Bull) ; Version 9.5.8;
  - Le serveur d'horodatage, permettant de délivrer des jetons d'horodatage de test pour les signatures augmentées. Ce serveur d'horodatage est représenté par une instance de MetaTIME (produit Bull) ; version 9.5.8;

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

1.4.3.2 Architecture de test

L'architecture suivante sera utilisée pour tester la TOE :



1.4.3.3 Dispositif de création de signature

Le dispositif de création de signature électronique utilisée par la TOE est hors périmètre d'évaluation. Ce dispositif est le seul à posséder la clé privée du signataire et à pouvoir l'utiliser. Ce dispositif dispose d'un fournisseur de services cryptographique sous forme de CSP (Cryptographic Service Provider) ou de librairie PKCS#11 et peut être :

- Une carte à puce (à travers l'interface normalisée PKCS #11) ;
- Un token USB (à travers l'interface normalisée PKCS #11) ;
- Un HSM (à travers l'interface normalisée PKCS #11) ;
- Un fichier protégé (au format normalisé PKCS #12).

Pour l'évaluation, les tests sont effectués sur le poste utilisateur équipé d'un système d'exploitation Windows 7 et avec une cartes à puces qualifiées renforcée, Gemalto Carte à puce IDPrime MD 840).

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

2 Déclarations de conformité

2.1 Conformité aux critères communs

La cible de sécurité est strictement conforme aux référentiels Critères Commun suivants :

- Common Criteria for Information Technology Security Evaluation, Version 3.1 R3, part 2 .
- Common Criteria for Information Technology Security Evaluation, Version 3.1 R3, part 3.
- Evaluation Assurance Level 3 augmented with AVA_VAN.3, and ALC_FLR.3.

2.2 Conformité à un profil de protection

La cible de sécurité est conforme aux profils de protection par démonstration :

- « Application de création de signature électronique » [PP-ACSE-CCv3.1], version 1.7 du 2 mars 2011
- « Module de vérification de signature électronique » [PP-MVSE-CCv3.1], version 1.7 du 2 mars 2011

Les modifications apportées par rapport aux profils de protection sont indiqués dans la présente cible par bleu souligné pour les ajouts et ~~orange barré~~ pour les suppressions.

2.3 Conformité à un paquet d'assurance

Le niveau d'assurance visé est le niveau EAL3 augmenté des composants d'assurance AVA_VAN.3 et ALC_FLR.3.

Note : ce niveau d'assurance correspond aux exigences définies par l'ANSSI pour le niveau de qualification standard avec les critères communs version 3.1 [QUA_STD].

2.4 Argumentaire de conformité

Les spécificités de la présente cible de sécurité relativement aux profils de protection sont énoncées ci-après par thème (sujets, politiques de signature, présentation de document,…). De plus, à la fin, un tableau global présente l'ensemble des modifications par catégorie dans l'ordre des modifications.

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

2.4.1 Les sujets

Le rôle S.MCS.Signataire a été raffiné. Il est assuré par l'application utilisatrice sauf lorsqu'il est demandé au signataire son consentement explicite avant la signature des données

Le rôle S.MVS.Vérificateur a été raffiné. Il est assuré par l'application utilisatrice.

Le rôle S.Administrateur_De_Sécurité a été raffiné. Il est assuré par l'application appelante.

2.4.2 La présentation du document

Le profil de protection « Application de création de signature électronique » demande que dans le cas d'une contre-signature, on suppose que le signataire dispose d'un moyen de connaitre au moins l'identité du ou des signataires précédents, et aux mieux vérifie cette ou ces signatures.
La TOE ne permet pas la contre-signature, il est donc nécessaire d'apporter les modifications suivantes :

Catégorie	Nom de l'élément	Modification apportée	Commentaires
Hypothèse	H.MCS.Présentation _Du_Document	Précision	Le sujet qui interagit directement avec la TOE est l'application utilisatrice.
Hypothèse	H.MCS.Présentation_Signatures_Existantes	Suppression de l'hypothèse	La TOE ne supporte pas la contre-signature
Objectif	OE.TOE.Présentation_Document	Suppression du paragraphe concernant la prise en compte des contre-signatures	La TOE ne supporte pas la contre-signature

2.4.3 Format de Signature et données à signer

La TOE supporte différents formats de signature (CAdES, XAdES, PAdES) et signe des attributs.
Pour ce faire, des raffinements (précisions) ont été effectués :

Catégorie	Nom de l'élément	Modification apportée	Commentaires
Bien	B.MCS.Données_A_Signer	Précisions sur les attributs à signer	-

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

Bien	B.MCS.Données_A_Signer_Formatées	Précisions sur les formats de la signature	Signature XAdES, CAdES ou PAdES
Bien	B.MCS.Signature_Electronique	Précisions sur les attributs à signer	-
OSP	P.MCS.Export_Signature_Electronique	Précision sur le sujet et sur le format signature utilisé	Le sujet est l'application utilisatrice
Objectif	O.MCS.Export_Signature_Electronique	Précision suivant le format signature utilisé	-
Bien	B.MVS.Attributs_Signés	Précisions sur les attributs signés	-

2.4.4 Politique de Signature

Les profils de protection mentionnent que l'administrateur de sécurité est en charge de la gestion (création/modification) des politiques de signature applicables par la TOE.

Dans la présente TOE, la politique de signature est définie par l'application utilisatrice qui la passe en paramètre à la TOE. Les modifications suivantes ont donc été apportées :

Catégorie	Nom de l'élément	Modification apportée	Commentaires
Sujet	S.MCS.Signataire	Précision sur la politique de signature	La politique de signature est définie par l'application utilisatrice.
OSP	P.TOE.Administration	Précision sur la gestion des politiques de signature	La politique de signature est définie par l'application utilisatrice.
Objectif	O.Administration	Précision sur la gestion des politiques de signature	La politique de signature est définie par l'application utilisatrice.
Bien	B.TOE.Politique_De_Signature	Précision sur le contenu des politiques de signature	-
Exigence fonctionnelle de sécurité	FMT_MSA.1.1//Selected documents	Précision sur la gestion des attributs de signature	C'est l'application utilisatrice qui peut définir les attributs de signature sous la forme de paramètres d'entrée.
Exigence fonctionnelle de sécurité	FMT_MTD.1.1/Management of the signature policies	Raffinement	C'est l'application utilisatrice qui définit la politique de signature utilisée

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

2.4.5 Données de validation et Tiers de confiances externes

Les précisions suivantes ont été ajoutées concernant les données de validation fournies par des tiers de confiances :

Catégorie	Nom de l'élément	Modification apportée	Commentaires
Hypothèse	H.MVS.Tiers_De_Confiance_Sûr	Ajout	On suppose que les données retournées par les Tiers de confiance sont fiables (sûres).
Objectif	OE.TOE.MVS.Tiers_De_Confiance_Sûr	Ajout	Couverture hypothèse H.MVS.Tiers_De_Confiance_Sûr

2.4.6 Autres raffinements

Catégorie	Nom de l'élément	Modification apportée	Commentaires
Exigence fonctionnelle de sécurité	FDP_IFF.1.1/ Electronic signature export	Raffinement	Précision sur la nature des attributs de signature

2.4.7 Hypothèses sur la machine hôte

L'hypothèse suivante concernant la machine hôte a été modifiée, précisant que la machine hôte est sous la responsabilité d'une personne morale ou physique autre que le signataire. Et sur le rôle administrateur de sécurité, qui est pris en charge par l'application utilisatrice (en fournissant les politiques de signature à utiliser).
En conséquence l'objectif OE.TOE.Machine_Hôte a été modifié.

Catégorie	Nom de l'élément	Modification apportée	Commentaires
Hypothèse	H.Machine_Hôte	Précisions	Précision sur qui est responsable de la machine hôte sur laquelle la TOE s'exécute. Et sur le rôle administrateur de sécurité qui est pris en charge par l'application utilisatrice (en fournissant les politiques de signature à utiliser).
Objectif	OE.TOE.Machine_Hôte	Précision	Précision sur qui est responsable de la machine hôte sur laquelle la TOE

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

			s'exécute. Conséquence de la modification de l'hypothèse H.TOE.Machine_Hôte.

2.4.8 Assignement demandés par les profils de protection

Les assignements suivants ont été effectués conformément à ce qui est demandé dans les profils de protection :

Catégorie	Nom de l'élément	Modification apportée	Commentaires
Exigence fonctionnelle de sécurité	FDP_IFF.1.1/Signer's certificate import	Assignement	Autres attributs du certificat du signataire.
Exigence fonctionnelle de sécurité	FDP_IFF.1.2/Signer's certificate import	Assignement	Autres attributs du certificat du signataire.
Exigence fonctionnelle de sécurité	FPT_TDC.1.2/Signer's certificate	Assignement	Ajout de règles d'interprétation d'un certificat
Exigence fonctionnelle de sécurité	FMT_SMF.1.1/ Management of the signature policies	Assignement	Opération possible : « define »
Exigence fonctionnelle de sécurité	FDP_IFF.1.1/Certification path	Assignement	Précision sur les données de révocation utilisées pour vérifier chaque certificat du chemin de certification.
Exigence fonctionnelle de sécurité	FPT_TDC.1.2/Electronic Signature	Assignement	Précisions sur les standards supportés (XAdES, CAdES, PAdES).
Exigence fonctionnelle de sécurité	FPT_TDC1.2/Time Reference	Assignement	Précision sur les standards supportés (RCF 3161).
Exigence fonctionnelle de sécurité	FPT_TDC.1.2/Certificates	Assignement	Précisions sur les standards supportés (RFC 5280, RFC 3739).
Exigence fonctionnelle de	FPT_TCD.1.2/Certificate revocation data	Assignement	Précision sur les standards supportés (RCF 5280).

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

sécurité			
Exigence fonctionnelle de sécurité	FCS_COP.1.1/Signature Verification	Assignement	Précisions sur les algorithmes de signatures supportés (RSA) et taille de clés (2048)
Exigence fonctionnelle de sécurité	FCS_COP1.1/Hash	Assignement	Précisions sur les algorithmes de hash supportés (SHA-256, SHA-384 or SHA-512)

2.4.9 Récapitulatif des modifications

Cette section présente l'ensemble des modifications réalisées dans les profils sous la forme d'un tableau organisé par « catégorie » :

Catégorie	Nom de l'élément	Modification apportée	Commentaires
Bien	B.MCS.Données_A_Signer	Précisions sur les attributs à signer	-
Bien	B.MCS.Données_A_Signer_Formatées	Précision sur les formats de signature	Signature XAdES, CAdES ou PAdES
Bien	B.MCS.Signature_Electronique	Précisions sur les attributs à signer	-
Bien	B.MVS.Attributs_Signés	Précisions sur les attributs signés	-
Bien	B.TOE.Politique_De_Signature	Précision sur le contenu des politiques de signature	-
Bien	B.TOE.Correspondance_FormatDoc_Application	Raffinement éditoriale	Ajout pour préciser que l'on se place bien dans le contexte de la vérification de signature.
Sujet	S.MCS.Signataire	Précision l'origine de la politique de signature	La politique de signature est fournie à la TOE par l'application utilisatrice.
OSP	P.MCS.Export_Signature_Electronique	Précision sur le sujet et sur le format de signature	Le sujet qui interagit directement avec la TOE est l'application utilisatrice
OSP	P.TOE.Administration	Précision sur la	La politique de signature est

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

		gestion des politiques de signature	définie par l'application utilisatrice.
Hypothèse	H.Machine_Hôte	Précisions	Précision sur qui est responsable de la machine hôte sur laquelle la TOE s'exécute. Et sur le rôle administrateur de sécurité qui est pris en charge par l'application utilisatrice (en fournissant les politiques de signature à utiliser).
Hypothèse	H.MCS.Présentation _Du_Document	Précision	Le sujet qui interagit directement avec la TOE est l'application utilisatrice.
Hypothèse	H.MCS.Présentation_Signatures_Existantes	Suppression	La TOE ne supporte pas la contre-signature.
Hypothèse	H.MVS.Tiers_De_Confiance_Sûr	Ajout	On suppose que les données retournées par les Tiers de confiance sont fiables (sûres).
Objectif	O.Administration	Précision sur la gestion des politiques de signature	La politique de signature est définie par l'application utilisatrice.
Objectif	O.MCS.Export_Signature_Electronique	Précision suivant le format de signature utilisé	-
Objectif	OE.TOE.Machine_Hôte	Précision	Précision sur qui est responsable de la machine hôte sur laquelle la TOE s'exécute. Conséquence de la modification de l'hypothèse H.TOE.Machine_Hôte.
Objectif	OE.TOE.Présentation_Document	Précision sur le sujet et suppression du paragraphe concernant le support de la contre-signature.	Précision sur le sujet interagissant directement avec la TOE : l'application utilisatrice. Suppression du paragraphe concernant la contre-signature, car la TOE ne la supporte pas. Conséquence de la modification des hypothèses : - H.MCS.Présentation _Du_Document - H.MCS.Présentation_Signatures_Existantes
Objectif	OE.TOEMVS.Tiers_De_Confiance_Sûr	Ajout	Ajout de cet objectif pour couvrir l'hypothèse H.MVS. Tiers_De_Confiance_Sûr.
Exigence	FMT_MSA.1.1/Selected	Précision sur la	C'est l'application utilisatrice qui

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

fonctionnelle de sécurité	documents	gestion des attributs de signature	peut définir les attributs de signature sous la forme de paramètres d'entrée.
Exigence fonctionnelle de sécurité	FDP_IFF.1.1/Signer's certificate import	Assignement	Autres attributs du certificat du signataire.
Exigence fonctionnelle de sécurité	FDP_IFF.1.2/Signer's certificate import	Assignement	Autres attributs du certificat du signataire.
Exigence fonctionnelle de sécurité	FPT_TDC.1.2/Signer's certificate	Assignement	Ajout de règles d'interprétation d'un certificat
Exigence fonctionnelle de sécurité	FDP_IFF.1.1/ Electronic signature export	Raffinement	Précision sur la nature des attributs de signature
Exigence fonctionnelle de sécurité	FMT_MTD.1.1/Management of the signature policies	Raffinement	C'est l'application utilisatrice qui définit la politique de signature utilisée
Exigence fonctionnelle de sécurité	FMT_SMF.1.1/ Management of the signature policies	Assignement	Opération possible : « define »
Exigence fonctionnelle de sécurité	FDP_IFF.1.1/Certification path	Assignement	Précision sur les données de révocation utilisées pour vérifier chaque certificat du chemin de certification.
Exigence fonctionnelle de sécurité	FPT_TDC.1.2/Electronic Signature	Assignement	Précisions sur les standards supportés (XAdES, CAdES, PAdES).
Exigence fonctionnelle de sécurité	FPT_TDC1.2/Time Reference	Assignement	Précision sur les standards supportés (RCF 3161).
Exigence fonctionnelle de sécurité	FPT_TDC.1.2/Certificates	Assignement	Précisions sur les standards supportés (RFC 5280, RFC 3739).
Exigence fonctionnelle de sécurité	FPT_TCD.1.2/Certificate revocation data	Assignement	Précision sur les standards supportés (RCF 5280).
Exigence fonctionnell	FCS_COP.1.1/Signature Verification	Assignement	Précisions sur les algorithmes de signatures supportés (RSA) et

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

e de sécurité			taille de clés (2048)
Exigence fonctionnelle de sécurité	FCS_COP1.1/Hash	Assignement	Précisions sur les algorithmes de hash supportés (SHA-256, SHA-384 or SHA-512)
Exigence fonctionnelle de sécurité	FMT_SMR.1.1/Security roles	Modification	Le rôle administrateur est supprimé car la TOE n'implémente pas ce rôle. Les politiques de signature utilisées pour la validation de signatures sont fournies par les applications utilisatrices en paramètre de l'appel. Seul le rôle « verifier » est conservé
Exigence fonctionnelle de sécurité	FIA_UID.2/ User Identification before any action	Modification	En conséquence de la modification de FMT_SMR.1.1/Security roles, qui ne contient plus qu'un seul rôle, il n'est pas nécessaire d'authentifier les applications clientes de la TOE lorsque celles-ci demandent la validation d'une signature électronique conformément à une politique de validation que l'application utilisatrice fournie.

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

3 Définition du problème de sécurité

3.1 Biens

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

3.1.1 Biens à protéger par la TOE (User data)

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

3.1.1.1 Biens spécifiques au module de création de signature (MCS)

Modules de création de signature – Document à signer

B.MCS.Ensemble_Des_Documents_A_Signer
L'ensemble des documents à signer lors de l'invocation du processus de signature peut être composé de: o soit un unique document électronique o soit plusieurs documents électroniques On entend ici par document: o soit simplement un document électronique o soit un document électronique avec une ou plusieurs signatures imbriquées attachées au document.
Protection: intégrité,

Modules de création de signature – Représentations des données à signer

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

Elles requièrent une protection en intégrité.

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

B.MCS.Données_A_Signer
Les données à signer sont les informations sur lesquelles portera la signature. o Le document à signer sélectionné par le signataire explicitement o Les attributs de la signature sélectionnés par le signataire explicitement ou implicitement par l'application. Les attributs de la signature comportent les données suivantes : o Le certificat du signataire o Une référence non ambiguë du certificat du signataire (DN de l'AC et numéro de série, condensat du certificat) o La référence à la politique de signature o Le type d'engagement (si spécifié), o Le rôle du signataire (si spécifié) o Le lieu présumé de la signature (si spécifié) o La date et l'heure présumées de la signature à partir de l'heure système de la machine hôte o Le format du document (type MIME)
Protection: intégrité,

B.MCS.Données_A_Signer_Formatées
Ces données correspondent à un premier formatage des données à signer (enveloppe PAdES, XAdES ou CAdES).
Protection: intégrité,

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

B.MCS.Condensé_Des_Données_A_Signer
Cette donnée est un condensé des données à signer formatées.
Protection: intégrité

B.MCS.Condensé_Formaté
Ce bien correspond au condensé des données à signer après avoir subi un formatage, préalablement à son envoi vers le SCDev.
Protection: intégrité

Modules de création de signature – Données retournées par la TOE

B.MCS.Signature_Électronique
La signature électronique est une enveloppe comprenant: - Le condensé de l'ensemble des données à signer; - La signature numérique; - Des informations supplémentaires pouvant faciliter la vérification de signature (attributs signés tel que : Certificat du signataire, identifiant de la politique de signature, algorithme de signature, algorithme de canonicalization) Ce bien doit être à protégé par la TOE au cours de sa constitution avant qu'il soit transmis au signataire.
Protection: intégrité

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

3.1.1.2 Biens spécifiques au module de vérification de signature (MVS)

Module de vérification de signature – Données en entrée

B.MVS.Document
Le document est le document signé par le signataire et pour lequel la TOE doit vérifier la signature. Il peut être fourni à la TOE soit dans le même fichier que la signature soit dans un fichier indépendant.
Protection: intégrité

B.MVS.Signature
La signature électronique d'un signataire sur le document.
Protection: intégrité

B.MVS.Attributs_Signés
Les attributs signés sont des données signées en même temps que le document. Elles fournissent au vérificateur des précisions relatives à la signature et aux circonstances dans lesquelles elle a été effectuée. Les attributs signés comprennent: - La référence non ambiguë du certificat du signataire (DN du certificat – Emetteur – Numéro de série du certificat) ou le certificat du signataire lui-même En option: - La référence à 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 à partir de l'heure système de la machine hôte - Le lieu présumé de signature, - Le format du document (type MIME) -

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

Protection: intégrité

B.MVS.Données_De_Validation_En_Entrée
Les données de validation sont les données utiles à la vérification, elles conprennent ~~peuvent comprendre~~: - Le certificat du signataire, - Des certificats d'AC, d'émetteurs de CRL, de réponses OCSP, d'unités d'horodatage,... - Des listes de certificats révoqués (CRL) ou des réponses OCSP ~~- Des réponses OCSP~~ - Des listes d'autorité de certification révoquées (ARL) - Des tampons d'horodatage Ces données peuvent être obtenues de plusieurs manières: - elles peuvent être obtenues d'un serveur distant (sur un réseau local ou ouvert), - elles peuvent être stockées en local sur la machine où la vérification est effectuée, - elles peuvent être stockées avec la signature (en fonction du format).
Protection: intégrité

Module de vérification de signature – Données de travail

B.MVS.Données_A_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.
Protection: intégrité

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

Module de vérification de signature – Données en sortie

B.MVS.Statut_De_Retour
Après la vérification, la TOE retourne un statut de vérification qui dépend du résultat. - 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 de la vérification immédiate, une validation incomplète doit être comprise par le vérificateur soit comme une signature invalide, soit comme la possibilité de tenter ultérieurement une nouvelle vérification immédiate. Dans le cas de la vérification ultérieure, une validation incomplète doit être comprise par le vérificateur comme une signature invalide.
Protection: intégrité

B.MVS.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 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.
Protection: intégrité

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

3.1.2 Biens sensibles de la TOE (TSF data)

Biens sensibles de la TOE (TSF data) – données partagées entre les modules

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

B.TOE.Politique_De_Signature
Les politiques de signature définissent les règles à appliquer pour créer et 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 (assuré par l'application utilisatrice) de la TOE, doit être protégée en intégrité. De plus, l'intégrité de chacune des politiques de signature doit aussi être contrôlée. Une politique de signature comprend les éléments suivants : o Le nom et la description textuelle de la politique de signature ; o L'identifiant unique (OID) de la politique de signature ; o L'identifiant des fonctions de hachage utilisables ; o Les certificats des AC Racines de confiances autorisées pour le certificat du signataire ; o Les valeurs autorisées de l'extension « certificatePolicies » du certificat du signataire et de la racine ; o Tests de la révocation du certificat du signataire et de la validité des CRLs ; o Les valeurs autorisées de l'extension « keyUsage » du certificat du signataire : présence des bits digital signature et non répudiation ; o Période de grâce pour le certificat du signataire ; o Les types d'engagements acceptés et le type choisi par défaut ; o Les certificats des AC Racines de confiances autorisées pour le certificat de l'autorité d'horodatage ; o Les valeurs autorisées de l'extension « certificatePolicies » du certificat de l'autorité d'horodatage ; o Tests de la révocation du certificat de l'autorité d'horodatage et de la validité des CRLs ; o Période de grâce pour le certificat de l'autorité d'horodatage.
Protection: intégrité

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

B.TOE.Services
Ce bien représente le code exécutable implémentant les services rendus.
Protection: intégrité

B.TOE.Correspondance_Données_Internes/Externes
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.
Protection: intégrité

B.TOE.Correspondance_FormatDoc_Application
Ce bien est un paramètre géré par la TOE qui lui permet de décider quelle application de présentation externe lancer en fonction du format du document devant être présenté au signataire ou au vérificateur. Dans le contexte de la vérification de signature, le format du document est: - soit fourni par le vérificateur, - soit présent dans la signature en tant qu'attribut signé.
Protection: intégrité

Biens sensibles de la TOE (TSF data) – donnée spécifique au module de vérification de signature (MVS)

B.TOE.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 implantant ces règles dans l'application requiert une protection en intégrité.
Protection: intégrité

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

3.2 Sujets

S.MCS.Signataire

Le signataire interagit avec la TOE pour signer un ou plusieurs documents selon une politique de signature définie par l'application utilisatrice.

Note :

Dans la présente cible d'évaluation, le rôle de signataire est assuré par l'application utilisatrice sauf lorsqu'il est demandé au signataire son consentement explicite avant la signature des données.

S.MVS.Vérificateur

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

Note :

Dans la présente cible d'évaluation, le rôle de signataire est assuré par l'application appelante

S.TOE.Administrateur_De_Sécurité

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

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

Note d'application

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

Note :

Dans la présente cible d'évaluation, le rôle Administrateur_De_Securité est assuré par l'application utilisatrice.

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

3.3 Menaces

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

3.4 Politiques de sécurité organisationnelles (OSP)

Cette section définit les règles applicables à la TOE.

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

P.TOE.Conformité_Certificat_Signataire
[MCS] Pour éviter la création de signatures invalides, la TOE doit contrôler que le certificat sélectionné par le signataire est bien conforme à la politique de signature à appliquer. [MVS] 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.

P.TOE.Validité_Certificat_Signataire
[MCS] Pour éviter la création de signatures invalides, la TOE doit contrôler que le certificat sélectionné par le signataire est bien utilisé durant sa période de validité. [MVS] La TOE doit contrôler que le certificat du signataire était bien valide au moment où la signature a été positionnée dans le temps.

P.TOE.Conformité_Attributs_Signature
[MCS]Pour éviter la création de signatures invalides, la TOE doit contrôler: o que les attributs de signature sélectionnés par le signataire sont bien conformes à la politique de signature à appliquer, et o que tous les attributs de signature requis par la politique de signature sont présents. [MVS]La TOE doit contrôler: o que les attributs signés sont bien conformes à la politique de signature à appliquer, et o que tous les attributs de signature requis par la politique de signature sont présents.

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

3.4.1.1 Politiques spécifiques à la vérification de signature

P.MVS.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).

P.MVS.Authenticité/Intégrité_Données_Validation
La TOE doit contrôler l'authenticité de l'origine et l'intégrité des données de validation fournies.

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

3.4.2 Contrôle de l'invariance de la sémantique du document

P.TOE.Sémantique_Document_Invariante

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

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

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

3.4.3 Présentation du document et des attributs de signature au signataire

P.TOE.Possibilité_De_Présenter_Le_Document

La TOE doit permettre au signataire (respectivement : au vérificateur) d'accéder à une représentation fidèle du document à signer (respectivement : à vérifier) (Décret 2001-272, Art 5 alinéa c).

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

[MVS]Note d'application

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

P.MCS.Présentation_Attributs_De_Signature

La TOE doit permettre de présenter les attributs de signature (respectivement : les attributs signés) au signataire (respectivement : au vérificateur).

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

3.4.4 Conformité aux standards

P.TOE.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 l'ANSSI [CRYPTSTD].

P.MVS.Algorithmes_De_Signature
Les algorithmes cryptographiques supportés et les longueurs des clés mises en oeuvre 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 l'ANSSI [CRYPTSTD]. Note d'application Les clés utilisées doivent être conformes au référentiel de gestion de clés de l'ANSSI [KEYSSTD].

3.4.5 Interaction avec l'utilisateur (signataire ou vérificateur)

P.MCS.Signature_De_Plusieurs_Document
La TOE doit permettre d'enchaîner la signature d'un nombre fini de documents, ce nombre pouvant être éventuellement de un. Le consentement à signer donné par le signataire pour ce ou ces documents portera sur les mêmes attributs de signature.

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

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

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

3.4.6 Contraintes diverses liées à la création de signature

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

P.MCS.Export_Signature_Électronique
A l'issue du processus de signature, la TOE doit transmettre au signataire la signature électronique du document comprenant au moins: - La signature numérique du document; - Le condensé de l'ensemble des données à signer; - Une référence au certificat du signataire ou le certificat du signataire lui-même ; - Une référence à la politique de signature appliquée Note d'application : D'autres informations facilitant la vérification de la signature peuvent être ajoutées (ex: le certificat du signataire in extenso, un tampon d'horodatage, etc.) Dans le cas d'une signature au format BES, la norme ETSI de ce format de signature ne permet d'inclure une référence à la politique de signature appliquée.

3.4.7 Contraintes diverses liées à la vérification de signature

P.MVS.Export_Données_Validation
La TOE doit permettre d'exporter au vérificateur les données de validation utilisées lors de la vérification.

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

3.4.8 Contraintes diverses liées à l'administration

P.TOE.Administration
La TOE doit permettre à l'administrateur de sécurité (assuré par l'application utilisatrice) de gérer: o [MCS & MVS] les politiques de signature [B.Politique_De_Signature] (ajouter/supprimer) o [MCS & MVS] la table de correspondance entre les applications de visualisation et les formats de documents en entrée de la TOE [B.Correspondance_FormatDoc_Application]. o [MVS] ainsi que d'inhiber la fonction de visualisation du document signé.

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

3.5 Hypothèses

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

3.5.1 Hypothèses sur l'environnement d'utilisation

3.5.1.1 Hypothèses sur la machine hôte

H.Machine_Hôte
On suppose que la machine hôte sur laquelle la TOE s'exécute est ~~soit directement sous la responsabilité du 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: o la machine hôte est protégée contre les virus o 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 o l'accès aux fonctions d'administration de la machine hôte est restreint aux seuls administrateurs de celle-ci (différenciation compte utilisateur/administrateur) o l'installation et la mise à jour de logiciels sur la machine hôte est sous le contrôle de l'administrateur o le système d'exploitation de la machine hôte refuse l'exécution d'applications téléchargées ne provenant pas de sources sûres Note d'application 1) Le rôle d'administrateur de la machine hôte mentionné ci-dessus est distinct de celui d'administrateur de sécurité de la TOE / l'application utilisatrice. 2) 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.

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

.

3.5.1.2 Création de signature – Hypothèses relatives au dispositif de création de signature

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

H.MCS.Dispositif_De_Création_De_Signature

On suppose que le SCDev a notamment pour fonction de générer effectivement la signature à partir des éléments communiqués par la TOE.

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

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

Les données suivantes sont supposées être stockées et utilisées de manière sûre par le SCDev:

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

(1) A noter que l'association peut porter sur une donnée d'authentification et un couple clé privée/certificat. Ainsi, plusieurs couples peuvent être stockés dans le même SCDev.

On peut imaginer que leur accès soit protégé par des données d'authentification différentes.

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

H.MCS.Communication_TOE/SCDev

On suppose que l'ensemble des composants logiciels et/ou matériels assurant l'interface entre la TOE et le SCDev est capable de gérer (ouvrir / fermer) un canal de communication garantissant l'intégrité et l'exclusivité de la communication.

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

H.MCS.Authentification_Signataire

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

3.5.1.3 Présentation du document

H.MCS.Présentation_Du_Document

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

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

~~**H.MCS.Présentation_Signatures_Existantes**~~

~~Dans le cas d'une contre-signature, on suppose que le signataire dispose d'un moyen de connaître au moins l'identité du ou des signataires précédents, et au mieux vérifie cette ou ces signatures.~~

La TOE ne permet pas la contre-signature.

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

3.5.1.4 Hypothèse concernant l'invariance de la sémantique du document

H.MCS.Contrôle_Invariance_Sémantique_Document
On suppose que l'environnement de la TOE fournit un module capable de déterminer si la sémantique du document à signer est bien invariante et de communiquer le statut de son analyse à la TOE.

3.5.2 Hypothèses sur le contexte d'utilisation

H.TOE.Politique_Signature_D'Origine_Authentique
L'origine de la ou des politiques de signature utilisables par la TOE est supposée authentique. Note d'application : 1) 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. 2) Cette hypothèse est remplie de facto si la TOE n'utilise pas de politiques de signature interprétées mais des politiques fixes.

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

H.MVS.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.

H.TOE.Administrateur_De_Sécurité_Sûr
L'administrateur de sécurité de la TOE est supposé être de confiance, formé à l'utilisation de la TOE

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

et disposant des moyens nécessaires à la réalisation de son activité.

Note :

Le rôle d'administrateur de sécurité étant assuré par l'application appelante, celle-ci est supposée être de confiance.

H.MCS.Intégrité_Services

L'environnement de la TOE est supposé fournir à l'administrateur de sécurité (ici l'application utilisatrice) les moyens de contrôler l'intégrité des services et des paramètres de la TOE.

H.MVS.Tiers_De_Confiance_Sûr

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

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

4 Objectifs de sécurité

4.1 Objectifs de sécurité pour la TOE

4.1.1 Objectifs de sécurité communs au module de création de signature et au module de vérification de signature

4.1.1.1 Objectifs généraux

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

4.1.1.2 Présentation du ou des documents à signer ou signés

O.Lancement_d'Applications_De_Présentation
La TOE devra pouvoir lancer une application externe pour permettre au signataire de visualiser le document à signer ou pour permettre au vérificateur de visualiser le document dont la signature est à vérifier. Pour identifier quelle application de présentation lancer, la TOE devra gérer la correspondance entre des formats pour lesquels elle autorise la signature et des applications externes. Dans le cadre de la vérification de signature, la TOE se basera sur l'indication du format du document fournie dans la signature électronique à vérifier. La TOE ne devra pas permettre la signature d'un document si elle ne peut déterminer quelle application de visualisation lancer. Un paramètre de configuration permettra à un administrateur (assuré par l'application utilisatrice) de la TOE de désactiver cette fonction au moment de l'installation de la TOE si l'utilisateur est une machine.

Note : La TOE prendra toutefois en charge la visualisation des fichiers texte. Pour tous les autres cas, le module externe d'affichage du document est de confiance, c'est à dire qualifié par l'ANSSI, ou ayant

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

fait l'objet d'une étude de sécurité ou d'une évaluation acceptées et reconnues par l'autorité d'homologation du système cible utilisant la TOE.

4.1.1.3 Conformité aux standards

O.Support_Cryptographique
La TOE devra supporter des algorithmes cryptographiques ayant les propriétés suivantes: o les algorithmes de hachage ne permettent pas de créer deux documents produisant le même condensé. o 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 l'ANSSI [CRYPTSTD]. Note d'application Les clés utilisées doivent être conformes au référentiel de gestion de clés de l'ANSSI [KEYSSTD].

4.1.2 Objectifs de sécurité pour le Module de Création de Signature (MCS)

4.1.2.1 Objectifs généraux

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

4.1.2.2 Interaction avec le signataire

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

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

attributs qui seront signés.

O.Consentement_Explicite

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

O.Abandon_Du_Processus_De_Signature

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

O.Ensemble_De_Documents_A_Signer

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

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

4.1.2.3 Application d'une politique de signature

O.Conformité_Du_Certificat

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

O.Validité_Du_Certificat

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

Note d'application

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

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

O.Conformité_Des_Attributs

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

O.Export_Signature_Électronique

A l'issue du processus de signature, la TOE devra transmettre au signataire (ici l'application utilisatrice) la signature électronique du document comprenant au moins (suivant le format de signature utilisé) :

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

Note d'application :

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

Dans le cas d'une signature au format BES, la norme ETSI de ce format de signature ne permet d'inclure une référence à la politique de signature appliquée.

4.1.2.4 Contrôle de l'invariance de la sémantique du document

O.Contrôle_Invariance_Document

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

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

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

o Soit la politique de signature impose de stopper le processus de signature et la TOE doit alors

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

stopper le processus;

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

Note : Le module externe de contrôle d'invariance doit être de confiance, c'est à dire soit qualifié par l'ANSSI, ou avoir fait l'objet d'une étude de sécurité ou d'une évaluation acceptées et reconnues par l'homologateur du système cible utilisant la TOE.

4.1.3 Objectifs pour le Module de Vérification de Signature (MVS)

4.1.3.1 Objectifs sur les règles de vérification

O.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 sure 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:

o un tampon d'horodatage signé par une entité de confiance, conformément à la

politique de signature,

o une marque de temps fournie par un acteur de confiance, conformément à la politique de signature.

O.Chemin_De_Certification

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

o le certificat du signataire dont la référence est fournie dans les attributs signés, et

o un point de confiance référencé dans la politique de signature.

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

O.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.

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

O.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.

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

4.1.3.2 Objectifs relatifs à la visualisation des données signées

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

O.Communication_Attributs_Signés
La TOE devra permettre de communiquer les attributs signés au vérificateur. 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).

O.Export_Données_Validation
La TOE devra permettre d'exporter au vérificateur les données de validation utilisées lors de la vérification.

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

O.Invocation_Module_Controle_Invariance
Pour chaque document, la TOE devra interroger un module externe 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).

Note : Le module externe de contrôle d'invariance doit être de confiance, c'est à dire soit qualifié par l'ANSSI, avoir fait l'objet d'une étude de sécurité ou d'une évaluation acceptées et reconnues par l'homologateur du système cible utilisant la TOE.

4.2 Objectifs de sécurité pour l'environnement opérationnel

4.2.1 Machine hôte

OE.TOE.Machine_Hôte
La machine hôte sur laquelle la TOE s'exécute devra être ~~soit directement sous la responsabilité du~~

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

~~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 que les mesures suivantes devront être appliquées:

o la machine hôte est protégée contre les virus;

o 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;

o l'accès aux fonctions d'administration de la machine hôte est restreint aux seuls administrateurs de celle-ci (différenciation compte utilisateur/administrateur);

o l'installation et la mise à jour de logiciels sur la machine hôte est sous le contrôle de l'administrateur;

o le système d'exploitation de la machine hôte refuse l'exécution d'applications téléchargées ne provenant pas de sources sûres.

~~Note d'application~~

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

4.2.2 Objectifs relatifs au SCDev et à son environnement

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

OE.MCS.Dispositif_De_Création_De_Signature

Le SCDev électronique devra avoir au moins pour fonction de générer effectivement la signature à partir des éléments communiqués par la TOE. De plus, il sera en charge de l'authentification du signataire pour lui permettre ou non d'utiliser la clé privée correspondant au certificat sélectionné.

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

Les données suivantes seront stockées et utilisées de manière sûre par le SCDev:

- Biens relatifs à la génération de la signature
  - o la(les) clé(s) privée(s) du signataire, protégée(s) en confidentialité et en intégrité
  - o le(s) certificat(s) du signataire, protégé(s) en intégrité, à défaut une référence non ambiguë à ce(s) certificat(s),
  - o l'association clé privée/certificat, protégée en intégrité

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

- Biens relatifs à l'authentification du signataire
  - les données d'authentification du signataire, protégées en intégrité et en confidentialité.
  - l'association entre des données d'authentification et le couple clé privée/certificat, protégée en intégrité

OE.MCS.Communication_TOE/SCDev

L'ensemble des composants logiciels et/ou matériels assurant l'interface entre la TOE et le SCDev devra être capable de gérer (ouvrir / fermer) un canal de communication garantissant l'intégrité et l'exclusivité de la communication.

OE.MCS.Protection_Données_Authentification_Signataire

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

4.2.3 Création de signature – Présence du signataire

OE.MCS.Présence_Du_Signataire

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

Note d'application

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

4.2.4 Global – Présentation/sémantique invariante du ou des documents à signer

OE.TOE.Présentation_Document

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

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

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

~~Dans le cas où le document à signer contient déjà des signatures l'environnement de la TOE permettra au signataire au moins de connaître les précédents signataires, au mieux de contrôler la validité des signatures.~~

Note : La TOE ne permet pas la contre signature. Ces applications de visualisation sont de confiance, c'est à dire qualifiées par l'ANSSI, ou ayant fait l'objet d'une étude de sécurité ou d'une évaluation acceptées et reconnues par l'autorité d'homologation du système cible utilisant la TOE.

OE.TOE.Contrôle_Sémantique_Document_Signer

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 : Ce module est de confiance, c'est à dire qualifié par l'ANSSI, ou ayant fait l'objet d'une étude de sécurité ou d'une évaluation acceptées et reconnues par l'autorité d'homologation du système cible utilisant la TOE.

4.2.5 Divers

OE.TOE.Administrateur_De_Sécurité_Sûr

L'administrateur de sécurité (assuré par l'application utilisatrice) de la TOE est de confiance, formé à l'utilisation de la TOE et dispose des moyens nécessaires à la réalisation de son activité

OE.TOE.Authenticité_Origine_Politique_Signature

Les administrateurs (ici assuré par l'application utilisatrice) de la TOE devront s'assurer de

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

l'authenticité de l'origine des politiques de signature avant qu'elles ne soient utilisées par la TOE.

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

OE.TOE.MVS.Tiers_De_Confiance_Sûr
Les serveurs des IGC et serveurs d'horodatage auxquels la TOE fait appel, doivent fournir des informations considérées fiables.

4.2.6 Vérification de signature – objectifs sur l'environnement spécifiques

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

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

5 Définition de composants étendus

Aucun composant étendu n'est nécessaire pour cette cible de sécurité.

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

6 Exigences de sécurité

6.1 Exigences de sécurité fonctionnelles pour la TOE

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

- Raffiné éditorialement (terme défini dans le [CC1]): raffinement dans lequel une modification mineure est faite sur un élément d'exigence, telle que la reformulation d'une phrase pour des raisons de respect de la grammaire anglaise. En aucun cas, cette modification ne doit changer la signification de l'exigence.
- Raffinement: raffinement qui permet d'ajouter des précisions ou de limiter l'ensemble des implémentations acceptables pour un élément d'exigence ou à tous les éléments d'exigences d'un même composant.

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

6.1.1 Exigences de sécurité fonctionnelles pour le Module de Création de Signature (MCS) de la TOE

Le tableau suivant liste les sujets, les objets, les opérations et leurs attributs de sécurité utilisés dans la formulation des exigences de sécurité fonctionnelles :

Subject	Object /Information	Operation	Security attributes
the Signer	a document to be signed	import of the document in the TOE	**the Signer**: - signature policy - signer's explicit agreement to sign the document if is not stable **a document to be signed:** - document's identifier - document's stability status
the Signer	the signer's certificate	import of the signer's certificate into the TOE	**the Signer:** - applied signature policy **the signer's certificate:** - key usage status - QCStatement if required by the signature policy - certificate identifier
- the Signer - theSCDev	- the data to be signed formatted - the electronic signature	transfert to the SCDev	**the Signer**: - applied signature policy - signer's certificate - signer's explicit agreement to sign the present non invariant document **the data to be signed formatted**: - the data to be signed format **the electronic signature:** - signature policy identifier - commitment type - claimed role - presumed signature date and time - presumed signature location
- the Signer - the SCDev	the electronic signature	export to the Signer	**the SCDev** - the status of signature generation process **the electronic signature:** - the generated electronic signature - the signed document's hash - the reference to the signer's certificate - the reference of the applied signature policy

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

6.1.1.1 Contrôle de l'invariance de la sémantique du document

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

Contrôle à l'import du document

FDP_IFC.1/Document acceptance for signature Subset information flow control

FDP_IFC.1.1/Document acceptance for signature The TSF shall enforce the [assignment] **document acceptance information flow control policy** on

[assignment]

- o **subjects: the signer,**
- o **information: a document to be signed**
- o **operation: import of the document in the TOE**.

FDP_IFF.1/Document acceptance for signature Simple security attributes

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

[assignment]

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

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

[assignment]

Import of the document:

- o **either the document's stability status equals "stable", or**

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

o **the document's stability status is "unstable" or "uncontrolled" but the signature policy allows to bypass the control and the signer explicitly acknowledges to bypass the control**.

FDP_IFF.1.3/Document acceptance for signature The TSF shall enforce the following [assignment] set of rules : none.

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

[assignment]

o **controls succeed**.

o **or controls bypassed.**

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

[assignment]

o **controls fail**.

o **and controls cannot be bypassed.**

Note d'application

La TOE devra fournir les moyens pour:

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

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

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

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

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

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

[assignment]

- o **determine whether the document's semantics is invariant or not by invoking a dedicated external module,**
- **o the document shall invoque an external module in charge of controlling that the semantics of the document to be signed is invariant,**
- **o the document shall inform the signer when the document's semantics is not stable.**

Raffinement:

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

Note d'application

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

FMT_MSA.3/Document's acceptance for signature Static attribute initialization

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

Raffinement:

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

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

FMT_MSA.1/Selected documents Management of security attributes

FMT_MSA.1.1/Selected documents The TSF shall enforce the [assignment] **document acceptance for signature information flow control policy** to restrict the ability to [selection] **select** the security attributes [assignment] **documents' to be signed identifiers** to [assignment] **the signer** (using application).

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

FMT_SMF.1/Selection of a list of documents Specification of Management Functions

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

[assignment]

- o **selecting a list of documents to be signed**.

Raffinement:

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

Note d'application

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

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

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

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

FMT_SMF.1/Getting document's semantics invariance status for signature Specification of Management Functions

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

[assignment]

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

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

FMT_MSA.1/Signer agreement to sign an instable document Management of security attributes

FMT_MSA.1.1/Signer agreement to sign an instable document The TSF shall enforce the [assignment] **document acceptance information flow control policy** to restrict the ability to [selection] **modify** the security attributes [assignment] **signer agreement to sign an instable document** to **the signer**.

FMT_SMF.1/Getting signer agreement to sign an instable document Specification of Management Functions

FMT_SMF.1.1/Getting signer agreement to sign an instable document The TSF

shall be capable of performing the following management functions:

[assignment]

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

6.1.1.2 Interaction avec le signataire

FDP_ROL.2/Abort of the signature process Advanced rollback

FDP_ROL.2.1/Abort of the signature process The TSF shall enforce [assignment] **the signature generation information flow control policy** to permit the rollback of [assignment] **all the operations** on the [assignment] **electronic signature and its related attributes.**

Application note : This SFR is realized through MetaSIGN-API usage

FDP_ROL.2.2/Abort of the signature process [Raffiné éditorialement] The TSF shall permit operations to be rolled back [assignment] **before the data to be signed formatted are transferred to the SCDev.**

6.1.1.3 Règles de validation

Règles relatives aux attributs de signature

Les exigences qui suivent se rapportent aux attributs de signature.

FMT_MSA.1/Signature attributes Management of security attributes

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

FMT_MSA.1.1/Signature attributes The TSF shall enforce the [assignment] **signature generation information flow control policy** to restrict the ability to [selection] **select** the security attributes **signature attributes** to [assignment] **the signer (assumed by using application).**

Application note :

Signature attributes taken into account by TOE are the following :

- **Signer certificate or its unique identifier ;**
- **Signing policy identifier ;**
- **Commitment type ;**
- **Signer rule ;**
- **Presence of Presumed date and hour of signature ;**
- **Presumed location of signature ;**

MIME type of document to sign.

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

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

[assignment]

> **o permit the signer (assumed by using application) to change the value of the signature attributes required by the applied signature policy.**

Raffinement:

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

Application note:

Calling application can permit the signer to change the value of the following signature attributes list when calling application:

- **Signer certificate ;**
- **Signing policy identifier ;**
- **Commitment type ;**
- **Signer rule ;**
- **Presence of Presumed date and hour of signature ;**
- **Presumed location of signature ;**
- **MIME type of document to sign.**

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

Règles relatives au certificat du signataire

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

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

Application note: The following FDP_IFC.1 SFRs are realized through MetaSIGN-API usage.

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

[assignment]

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

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

Application note: The following FDP_IFF.1 SFRs are realized through MetaSIGN-API usage.

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

[assignment]

- o **subjects: the signer (applied signature policy)**
- o **information: the signer's certificate (key usage, Signature SFP), the Certificate Authority of the signer's certificate, the validity period time of the signer's certificate**.

FDP_IFF.1.2/Signer's certificate import The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

[assignment]

Import of the signer's certificate into the TOE

- o **the "key usage" of the selected signer's certificate indicates that this certificate is usable for non repudiation purposes (Application note: bit 1 of keyUsage set)**
- o **the certificate is a Qualified Certificate if required by the signature policy (Application note: information available using a QCStatement, see RFC 3739),**

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

o **the private key corresponding to public key is protected by an SCDev (Application note: information available using a QCStatement, see RFC 3739)**.

- o **the certificate is issued by one of the Certificate Authorities defined by the calling application (through the signature policy),**
- o **the certificate is valid at time indicated by the time stamping service or by the system's time if no time stamping service is specified.**

Note d'application :

La TOE utilise des politiques de signature au format XML définie par [TR 102 038]. Ces politiques de signature n'ont pas la possibilité de requérir un certificat dit « qualifié » (disposant de l'information QCStatement)

FDP_IFF.1.3/Signer's certificate import The TSF shall enforce the **other rules explicitly defined in the Signature SFP (eventually including the QCStatement)**.

FDP_IFF.1.4/Signer's certificate import The TSF shall explicitly authorise an information flow based on the following rules:

[assignment]

o **controls succeed**.

FDP_IFF.1.5/Signer's certificate import The TSF shall explicitly deny an information flow based on the following rules:

[assignment]

o **controls fail**.

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

Application note: The following FDP_MSA.3 SFRs are realized through MetaSIGN-API usage.

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

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

FMT_MSA.1/Signer's certificate Management of security attributes

Application note: The following FMT_MSA.1 SFRs are realized through MetaSIGN-API usage.

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

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

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

Application note: The following FDP_ITC.2 SFRs are realized through MetaSIGN-API usage.

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

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

FDP_ITC.2.3/Signer's certificate The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4/Signer's certificate The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5/Signer's certificate The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [assignment] **none.**

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

Application note: The following FPT_TDC.1 SFRs are realized through MetaSIGN-API usage.

FPT_TDC.1.1/Signer's certificate The TSF shall provide the capability to consistently interpret [assignment] **certificates** when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/Signer's certificate The TSF shall use [assignment] **the following list of interpretation rules :**

- **interpretation of the key usage.**

when interpreting the TSF data from another trusted IT product.

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

Application note: The following FMT_SMF.1 SFRs are realized through MetaSIGN-API usage.

FMT_SMF.1.1/Signer's certificate selection The TSF shall be capable of performing the following management functions:

[assignment]

- **allow the signer to select a certificate among the list of certificates suitable for the applied signature policy**.

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

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

FDP_IFC.1/Signature generation Subset information flow control

Application note: The following FDP_IFC.1 SFRs are realized through MetaSIGN-API usage.

FDP_IFC.1.1/Signature generation The TSF shall enforce the [assignment] **signature generation information flow control policy** on

[assignment]

o subjects: the signer, the SCDev

o information:

- the data to be signed formatted

- the electronic signature (once generated)

o operations:

-transfert to the SCDev.

FDP_IFF.1/Signature generation Simple security attributes

Application note: The following FDP_IFF.1 SFRs are realized through MetaSIGN-API usage except for document viewer launching.

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

[assignment]

o subjects: the using application (applied signature policy) the signer (~~applied signature policy,~~ signer's certificate), signer's explicit agreement to sign the present non invariant document (see FDP_IFF.1.2/Signature generation), the SCDev ([assignment: SCDev's attribute] : no attribute used)

o information: the data to be signed formatted (the data to be signed format), the electronic signature (signature policy identifier, commitment type, claimed role, presumed signature date and time, presumed signature location,).

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

[assignment]

Transfer of the data to be signed formatted:

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

o communicate the signature attributes to the signer before the signature generation

o launch the viewer corresponding to the document's format according to the document format/viewer association table

o activate the signing key corresponding to the selected signer's certificate.

Electronic signature:

o if the signature policy requires the inclusion of the signature attribute "signature policy identifier", then its value shall be included;

o if the signature policy requires the inclusion of the signature attribute "commitment type", then its value shall be included;

o if the signature policy restricts the values to be taken by the "commitment type" attribute, then its value shall be conformant to the signature policy;

o if the signature policy requires the inclusion of the signature attribute "claimed role", then its value shall be included;

o if the signature policy restricts the values to be taken by the "claimed role" attribute then its value shall be conformant to the signature policy;

o if the signature policy prevents the inclusion of the signature attribute "presumed signature date and time", then its value shall not be included;

o if the signature policy requires the inclusion of the signature attribute "presumed signature location", then its value shall be included;

o none.

Note d'application :

La TOE utilise des politiques de signature au format XML des politiques de signature défini par [TR 102 038]. Les politiques de signature ont la possibilité de requérir :

- **L'inclusion de l'attribut de signature « signature policy identifier » représenté par l'information « SignaturePolicyIdentifier » dans la politique ;**
- **L'inclusion de l'attribut de signature « commitment type » représenté par l'information « CommitmentTypeIndication » dans la politique. Dans ce cas, la valeur devra être en conformité avec la liste présente dans la politique de signature ;**
- **L'inclusion de l'attribut de signature « claimed role » représenté par l'information « SignerRole » dans la politique. Cependant la politique ne peut pas en restreindre les valeurs ;**
- **L'inclusion de l'attribut de signature « presumed signature date and time » représenté par l'information « SigningTime » dans la politique ;**
- **L'inclusion de l'attribut de signature « presumed signature location » représenté par l'information « SignatureProductionPlace » dans la politique ;**

Les politiques de signature au format XML des politiques de signature défini par [TR 102 038] ne permettent pas d'interdire la présence de l'un de ces attributs

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

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

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

[assignment]

o Security attributes are compliant to Signature SFP

o and the data to be signed formatted semantic control succeed.

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

[assignment]

o Security attributes are not compliant to the Signature SFP

o or the data to be signed formatted semantic control fails.

Note d'application

La TOE doit fournir les moyens de:

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

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

FMT_MSA.3/Signature generation Static attribute initialisation

Application note: The following FMT_MSA.3 SFRs are realized through MetaSIGN-API usage.

FMT_MSA.3.1/Signature generation The TSF shall enforce the [assignment] **signature generation information flow control policy** to provide [selection] **restrictive** default values for security attributes that are used to enforce the SFP.

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

FDP_ITC.1/Explicit signer agreement Import of user data without security attributes

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

FDP_ITC.1.1/Explicit signer agreement The TSF shall enforce the [assignment] **signature generation information flow control policy** when importing user data, controlled under the SFP, from outside of the TOE.

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

FDP_ITC.1.3/Explicit signer agreement The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [assignment] **none**.

6.1.1.5 Retour de la signature électronique

FDP_IFC.1/Electronic signature export Subset information flow control

Application note: The following FDP_IFF.1 SFRs are realized through MetaSIGN-API usage.

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

[assignment]

- o **subjects:**
  - **-the signer,**
  - **-the SCDev**
- o **information:**
  - **-the electronic signature**
- o **operations:**
  - **-export to the signer**.

FDP_IFF.1/Electronic signature export Simple security attributes

Application note: The following FDP_IFF.1 SFRs are realized through MetaSIGN-API usage.

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

[assignment]

- o **subjects:**
  - **-the signer ([assignment: signer's security attributes] signer certificate, the reference to the signer's private key)**
  - **-the SCDev (the status of signature generation process, [assignment: any other SCDev attributes] : no attribute used)**

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

-using application

o **information:**

-the electronic signature (the generated electronic signature, the signed document's hash, the reference to the signer's certificate, the reference of the applied signature policy, [assignment: list of signature attributes] - all the signature attributes as defined in the supported standards (cf. section Erreur ! Source du renvoi introuvable.)~~none~~**).**

Note d'application :

La TOE permet la production de signatures sous différents formats d'augmentation. Dans ce cas, la signature est augmentée par des propriétés non signées contenant toutes les valeurs qui pourraient être nécessaires lors de la vérification (horodatage, certificats d'AC, CRLs).

Pour les formats suivants :

- **ES-T, les signatures contiennent :**
  - **un jeton d'horodatage (obtenu par requête auprès d'un service d'horodatage)**
- **ES-C, les signatures contiennent :**
  - **un jeton d'horodatage (obtenu par requête auprès d'un service d'horodatage)**
  - **les références des AC et CRLS associés au certificat du signataire et de l'horodatage**
- **ES-X Long ou LTV (cas de PAdES), les signatures contiennent :**
  - **un jeton d'horodatage (obtenu par requête auprès d'un service d'horodatage)**
  - **les références des AC et CRLS associés au certificat du signataire et de l'horodatage**
  - **les valeurs des AC et CRLS associés au certificat du signataire et de l'horodatage**
- **ES-A, les signatures contiennent :**
  - **un jeton d'horodatage (obtenu par requête auprès d'un service d'horodatage)**
  - **les références des AC et CRLS associés au certificat du signataire et de l'horodatage**
  - **les valeurs des AC et CRLS associés au certificat du signataire et de l'horodatage**
  - **un jeton d'archivage (obtenu par requête auprès d'un service d'horodatage)**

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

[assignment]

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

Export of the electronic signature to the signer is allowed if the signature generation (performed by the SCDev) succeeded.

FDP_IFF.1.3/Electronic signature export The TSF shall enforce the [assignment] **other rules explicitly defined in the signature policy**.

FDP_IFF.1.4/Electronic signature export The TSF shall explicitly authorise an information flow based on the following rules:

[assignment]

- o **Signature generation succeeds**.

FDP_IFF.1.5/Electronic signature export The TSF shall explicitly deny an information flow based on the following rules:

[assignment]

- o **Signature generation fails**.

FDP_ETC.2/Electronic signature export Export of user data with security attributes

FDP_ETC.2.1/Electronic signature export The TSF shall enforce the [assignment] **electronic signature export information flow control policy** when exporting user data, controlled under the SFP(s), outside of the TOE.

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

FDP_ETC.2.3/Electronic signature export The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.

FDP_ETC.2.4/Electronic signature export The TSF shall enforce the following rules when user data is exported from the TOE: [assignment] **none.** .

FMT_MSA.3/Electronic signature export Static attribute initialization

Application note: The following FMT_MSA.3 SFRs are realized through MetaSIGN-API usage.

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

FMT_MSA.3.2/Electronic signature export [Raffiné éditorialement] The TSF shall allow [assignment] **nobody** to specify alternative initial values to override the default values when an object or information is created.

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

FMT_MSA.1/SCDev signature generation status Management of security attributes

Application note: The following FMT_MSA.1 SFRs are realized through MetaSIGN-API usage.

FMT_MSA.1.1/SCDev signature generation status The TSF shall enforce the [assignment] **electronic signature export information flow control policy** to restrict the ability to [selection] **modify** the security attributes [assignment] **SCDev's signature generation status** to **nobody**.

FMT_SMF.1/Getting SCDev's signature generation status Specification of Management Functions

Application note: The following FMT_SMF.1 SFRs are realized through MetaSIGN-API usage.

FMT_SMF.1.1/Getting SCDev's signature generation status The TSF shall be capable of performing the following management functions:

[assignment]

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

6.1.1.6 Opération cryptographiques

FCS_COP.1/Hash function Cryptographic operation

Application note: The following FCS_COP.1 SFRs are realized through MetaSIGN-API usage.

FCS_COP.1.1/Hash function The TSF shall perform

- o [assignment] **hash generation** in accordance with a specified cryptographic algorithm **[assignment : cryptographic algorithm]** **SHA-256, SHA-384 or SHA-512** and cryptographic key sizes **[assignment : cryptographic size]** **none** that meet the following: [assignment] **CRYPT-STD, [assignment: list of standards]** **, FIPS 180-2**.

6.1.1.7 Identification et authentification de l'utilisateur

FMT_SMR.1/Signer security roles

FMT_SMR.1.1/The TSF shall maintain the roles

[assignment]

- o **the signer**

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

o **the security administrator** (assumed by using application).

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

FIA_UID.2/Signature User identification before any action

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

Note d'application

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

6.1.1.8 Administration de la TOE

Capacité à présenter le document au signataire

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

FMT_MTD.1.1/Document format/viewer association table The TSF shall restrict the ability to [selection] **modify** the [assignment] **document format/viewer association table** to [assignment] **the administrator** (assumed by using application).

FMT_SMF.1/Management of the document format/viewer association table for signature Specification of Management Functions

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

[assignment]

o **allow the administrator (assumed by the application using the TOE) to manage the document format/viewer association table**.

Gestion des politiques de signature

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

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

FMT_MTD.1.1/Management of the signature policies The TSF shall restrict the ability to [selection] **define** the [assignment] **signature policies** to [assignment] **the security administrator (assumed by using application) of the TOE**.

Note :

La politique de signature est transmise par l'application utilisatrice à la TOE lors de l'appel.

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

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

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

6.1.2 Exigences de sécurité fonctionnelles pour le Module de Vérification de Signature (MCS) de la TOE

Le tableau suivant liste les sujets, les objets, les opérations et leurs attributs de sécurité utilisés dans la formulation des exigences de sécurité fonctionnelles:

Subject	Object /Information	Operation	Security attributes
the Verifier	a signed document	import of the document in the TOE	**the Verifier:** - signature policy **the signed document:** - document's stability status
the Verifier	the electronic signature (the signature and the related signed attributes) and the signed document	import of the electronic signature	**the Verifier:** - applied signature policy **the electronic signature:** - signature policy - commitment type - claimed role - presumed signature date and time - presumed signature location **the signed document:** - the signed document's content format
the Verifier	the time reference applied to the signature	import of the time reference	**the Verifier:** - applied signature policy **the time reference applied to the signer's electronic signature:** - the root keys applicable to verify the time-stamp tokens - time-stamp unit certificate - any needed certificate between the certificate and the root key

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

Subject	Object /Information	Operation	Security attributes
the Verifier	- the certificates belonging to a certification path - the revocation data needed to validate the certification path	import of the certificates and the revocation data	**the Verifier:** - applied signature policy **the certificates belonging to a certification path** - key usage - QCStatement if required by the signature policy - the electronic signaturestatus "correct" - the period of validity of the certificate the time reference - certification policy
the Verifier	validation status « correct signature »	Communication of the status to the verifier	**validation status:** - signer's public key - document's hash - document's electronic signature

6.1.2.1 Contrôles à l'import du document

FDP_IFC.1/Document acceptance for verifying Subset information flow control

FDP_IFC.1.1/Document acceptance for verifying The TSF shall enforce the [assignment] **document acceptance for verifying information flow control policy** on

[assignment]

- o **subjects: the verifier,**
- o **information: a signed document**
- o **operation: import of the document in the TOE**.

FDP_IFF.1/Document acceptance for verifying Simple security attributes

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

[assignment]

- o **subjects: the verifier (signature policy),**
- o **information: the signed document (document's stability status)**.

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

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

[assignment]

Import of the document:

o **either the document's stability status equals "stable", or**

o **the document's stability status is "unstable" or "uncontrolled" but the signature policy allows to bypass the control and the verifier explicitly acknowledges to bypass the control**

The Verifier should be informed only if the document's semantics is unstable.

FDP_IFF.1.3/Document acceptance for verifying The TSF shall enforce the [assignment] **none**.

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

[assignment]

o **controls succeed**

o **or controls bypassed**.

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

[assignment]

o **controls fail**

o **and controls cannot be bypassed**.

Note d'application

La TOE devra fournir les moyens pour:

- o invoquer un vérificateur externe chargé de contrôler l'invariance de la sémantique du document à signer,
- o informer le signataire du document si la sémantique n'est pas stable

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

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

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

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

FDP_ITC.1.3/Document acceptance for verifying The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [assignment] **determine whether the document's semantics is invariant or not by invoking a dedicated external module**.

Raffinement:

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

Note d'application

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

FMT_MSA.3/Document's acceptance for verifying Static attribute initialisation

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

Raffinement:

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

FMT_MSA.3.2/Document's acceptance for verifying [Raffiné éditorialement] The TSF shall allow [assignment] **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 for verifying Management of security attributes

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

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

FMT_SMF.1/Getting document's semantics invariance status for verifying Specification of Management Functions

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

[assignment]

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

6.1.2.2 Présentation du document signé

FMT_SMF.1/Management of the document format/viewer association table for verifying Specification of Management Functions

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

[assignment]

o **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 [selection] **initialize** the [assignment] **viewer activation parameter** to [assignment] **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 management functions:

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

[assignment]

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

6.1.2.3 Politiques de signature

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 [selection] **select** the **applied signature policy** to [assignment] **the verifier (assumed by using 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 management functions:

[assignment]

o **the verifier (assumed by using application) shall be permitted to select the signature policy to be applied**.

6.1.2.4 Vérification de la signature

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

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

Application note: The following FDP_IFC.1 SFRs are realized through MetaSIGN-API usage.

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

[assignment]

o **subjects: the verifier,**

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

o **information: the electronic signature (the electronic signature and related signed attributes, and the signed document)**

o **operation: import of the electronic signature (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

Application note: The following FDP_IFF.1 SFRs are realized through MetaSIGN-API usage except for document viewer launching

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

[assignment]

o **subjects: the verifier (applied signature policy ([assignment: verifier's attributes] : none)**

o **information: the electronic signature (signature policy, commitment type, claimed role, presumed signature date and time, presumed signature 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:

[assignment]

Signature import:

o **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;**

o inform the verifier if the referenced signature policy is not the applied signature policy, when the electronic signature includes a reference to a signature policy.

o if the signed attribute "signature policy" is present in the electronic signature, then its value is conformant to the signature policy;

o if the signed attribute "commitment type" is present in the electronic signature, then its value is conformant to the signature policy;

o if the signed attribute "claimed role" is present in the electronic signature, then its value is conformant to the signature policy;

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

o if the signed attribute "presumed signature date and time" is present in the electronic signature, then its value is conformant to the signature policy;

o if the signed attribute "presumed signature location" is present in the electronic signature then its value is conformant to the signature policy

o none.

Note d'application :

La TOE utilise des politiques de signature au format XML des politiques de signature défini par [TR 102 038]. Les politiques de signature ont la possibilité de permettre le contrôle de conformité de :

- **L'attribut de signature « signature policy identifier » représenté par l'information « SignaturePolicyIdentifier » dans la politique lorsqu'il est présent dans la signature électronique ;**
- **L'attribut de signature « commitment type » représenté par l'information « CommitmentTypeIndication » dans la politique lorsqu'il est présent dans la signature électronique ;**
- **L'attribut de signature « claimed role » représenté par l'information « SignerRole » dans la politique lorsqu'il est présent dans la signature électronique. Cependant la politique ne peut pas en restreindre les valeurs ;**
- **L'attribut de signature « presumed signature location » représenté par l'information « SignatureProductionPlace » dans la politique lorsqu'il est présent dans la signature électronique ;**

La TOE utilise un viewer qui est toujours activé.

FDP_IFF.1.3/Electronic signature The TSF shall enforce the [assignment] **other rules explicitly defined in the Signature SFP.**

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

[assignment]

o the signed attributes are compliant with the Signature SFP

o and the signed document is stable.

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

[assignment]

o the signed attributes are not compliant with the Signature SFP

o or the signed document is unstable.

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

Note d'application

La TOE devra fournir les moyens pour:

- invoquer un vérificateur externe chargé de contrôler l'invariance de la sémantique du document à signer

FMT_MSA.3/Electronic signature Static attribute initialisation

Application note: The following FMT_MSA.3 SFRs are realized through MetaSIGN-API usage.

FMT_MSA.3.1/Electronic signature The TSF shall enforce the [assignment] **electronic signature access control policy** to provide [selection] **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

Application note: The following FDP_MSA.1 SFRs are realized through MetaSIGN-API usage.

FMT_MSA.1.1/Electronic signature The TSF shall enforce the [assignment] **electronic signature access control policy** to restrict the ability to [selection] **modify** the security attributes [assignment] **signature and its signed attributes** to [assignment] **nobody**.

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

Application note: The following FDP_ITC.2 SFRs are realized through MetaSIGN-API usage.

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

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 TOE:

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

[assignment]

- o **invoque an external 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).**
- o **transmit the result of the module's analysis to the verifier**.

Import d'une réference de temps valide

FDP_IFC.1/Time reference Subset information flow control

Application note: The following FDP_IFC.1 SFRs are realized through MetaSIGN-API usage.

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

[assignment]

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

FDP_IFF.1/Time reference Simple security attributes

Application note: The following FDP_IFF.1 SFRs are realized through MetaSIGN-API usage.

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

[assignment]

- o **subjects: the verifier (applied signature policy, [assignment: other verifier's attributes, if any] : none)**
- o **information: the time reference applied to the signer's electronic 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:

[assignment]

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

- o **the key usage of the time-stamping unit certificate indicates that this certificate is only usable for timestamping purposes**

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

o **there exists a certification path between the time-stamping unit certificate and a root certificate dedicated to the verification of timestamping tokens**

o **each rule applied to the previously mentioned certification path defined in requirement FDP_IFF.1/Certification path is met for the date/time included in the time reference**.

Application note:

As it is assumed that TOE is using a trusted timestamping service, the date/time included in the time reference is not checked.

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

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

o **controls succeed**.

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

[assignment]

o **controls fail**.

FMT_MSA.3/Time reference Static attribute initialisation

FMT_MSA.3.1/Time reference The TSF shall enforce the [assignment] **time reference acceptance access control policy** to provide [selection] **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 [assignment] **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 [Raffiné éditorialement] The TSF shall enforce the [assignment] **time reference acceptance flow control policy** to restrict the ability to [selection] **modify** the security attributes [assignment] **of the time reference** to [assignment] **nobody**.

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

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

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

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 TOE: [assignment] **none.**

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 [assignment] **certification path acceptance information flow control policy** to restrict the ability to [assignment] **modify** the security attributes [assignment] **of the imported certificates** to [assignment] **nobody**.

Données de validation des certificats

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

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

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

Divers

FDP_IFC.1/Certification path Subset information flow control

Application note: The following FDP_IFC.1 SFRs are realized through MetaSIGN-API usage.

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

[assignment]

- o **subjects: the verifier,**
- o **information:**
  - **-the certificates belonging to a certification path**
  - **-the revocation data needed to validate the certification path**
- o **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

Application note: The following FDP_IFF.1 SFRs are realized through MetaSIGN-API usage.

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

[assignment]

- o **subjects: the verifier (applied signature policy)**
- o **information: certification path validation data, including:**
  - **-the certificates belonging to the certification path (certificates' fields): key usage, QCStatement, the electronic signature status, the period of validity, the time reference, certification policy.**
  - **-the revocation data of each certificate in the certification path (revocation data's numeric signature, revocation data's revocation list),**
  - **-none.**

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

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,**

The following rules are met at the date/time included in the imported time reference.

Certification path:

- **for each certificate of the certification path, the electronic 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 electronic 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).**
- **[assignment: any other supported rule on signer's certificate fields] none.**

The following rules are met.

Signer's certificate:

- **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 if required by the signature policy (Application note: information available using a QCStatement, see RFC 3739),**
- **the private key corresponding to public key is protected by an SCDev (Application note: information available using a QCStatement, see RFC 3739)**
- **[assignment: any other supported rule on signer's certificate fields], none.**

Note d'application :

La TOE utilise des politiques de signature au format XML définie par [TR 102 038]. Ces politiques de signature n'ont pas la possibilité de requérir un certificat dit « qualifié » (disposant de l'information QCStatement)

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

FDP_IFF.1.3/Certification path The TSF shall enforce the [assignment] **none.**

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

[assignment]

o **controls succeed**.

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

[assignment]

o **controls fail**.

FMT_MSA.3/Certification path Static attribute initialisation

FMT_MSA.3.1/Certification path The TSF shall enforce the [assignment] **certification path acceptance information flow control policy** to provide [selection] **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 [assignment] **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 [assignment] **certification path acceptance information flow control policy** when importing user data, controlled under the SFP, from outside of the TOE.

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.

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

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

[assignment]

- **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**.

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

Application note: The following FPT_TDC.1 SFRs are realized through MetaSIGN-API usage.

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

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

- **CAdES : ETSI TS 101 733 (version 2.2.1) (2013-04) ;**
- **XAdES : ETSI TS 101 903 (version 1.4.2) (2010-12) ;**
- **PAdES : ETSI TS 102 778-2 (version 1.2.1) (2009-07), TS 102 778-3 (version 1.2.1) (2010-07) et TS 102 778-4 (version 1.1.2) (2009-12)**

when interpreting the TSF data from another trusted IT product.

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

Application note: The following FPT_TDC.1 SFRs are realized through MetaSIGN-API usage.

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

FPT_TDC.1.2/Time reference The TSF shall use [assignment] **the following standards:**

- **RFC 3161**

when interpreting the TSF data from another trusted IT product.

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

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

Application note: The following FPT_TDC.1 SFRs are realized through MetaSIGN-API usage.

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

FPT_TDC.1.2/Certificates The TSF shall use [assignment] **the following standards :**

- **RFC 5280**
- **RFC 3739**

when interpreting the TSF data from another trusted IT product.

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

Application note: The following FPT_TDC1 SFRs are realized through MetaSIGN-API usage.

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

FPT_TDC.1.2/Certificate revocation data The TSF shall use [assignment] **the following standards :**

- **RFC 5280**

when interpreting the TSF data from another trusted IT product.

Retour du statut de vérification

FDP_IFC.1/Electronic signature validation Subset information flow control

Application note: The following FDP_IFC.1 SFRs are realized through MetaSIGN-API usage.

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

[assignment]

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

FDP_IFF.1/Electronic signature validation Simple security attributes

Application note: The following FDP_IFF.1 SFRs are realized through MetaSIGN-API usage.

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

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

[assignment]

- o **subject: the verifier (the signed document)**
- o **information: validation status "correct signature" (represented technically by the value "true") (signer's public key, document's hash, document's electronic 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:

[assignment]

Communication of the status to the verifier:

- o **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;**
- o **the document's electronic signature, verified using the signer's public key, is correct**
- o **to communicate the status "~~wrong signature~~false " in case at least one rule among the information control policy rules is false**.
- o **to communicate the status "inderterminate" (represented technically by the value "null") in case at least one rule among the information control policy rules cannot be verified (i.e. one certificate or one CRL is missing).**

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

FDP_IFF.1.4/Electronic signature validation The TSF shall explicitly authorise an information flow based on the following rules:

[assignment]

- o **controls succeed**.

FDP_IFF.1.5/Electronic signature validation The TSF shall explicitly deny an information flow based on the following rules:

[assignment]

- o **controls fail**.

FMT_MSA.3/Signature validation status Static attribute initialisation

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

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

FMT_MSA.3.2/Signature validation status The TSF shall allow the [assignment] **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 [assignment] **electronic signature validation information flow policy** to restrict the ability to [selection] **modify** the security attributes [assignment] **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 [assignment] **electronic signature validation information flow policy** when exporting user data, controlled under the SFP(s), outside of the TOE.

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 TOE, 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 TOE:

[assignment]

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

-**the validation data contributing to prove the verification status correctness,**

-**the signed attributes, and**

-**the result of the analysis of the document's semantics invariance to the verifier**.

Note d'application

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

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

Les attributs signés et la stabilité de la sémantique du document sont communiqués au vérificateur par une interface programmatique ou une interface homme/machine.

6.1.2.5 Support cryptographique

FCS_COP.1/Signature verification Cryptographic operation

Application note: The following FCS_COP.1 SFRs are realized through MetaSIGN-API usage.

FCS_COP.1.1/Signature verification The TSF shall perform

[assignment]

o **electronic signature verification** in accordance with a specified cryptographic algorithm **[assignment: cryptographic algorithm]: RSA** and cryptographic key sizes **[assignment: cryptographic key sizes]** 2048 bits that meet the following: **CRYPT-STD, [assignment: list of standards] , PKCS#1.**

Note d'application

Les clés utilisées doivent être conformes au référentiel de gestion de clés de l'ANSSI [KEYSSTD].

FCS_COP.1/Hash Cryptographic operation

Application note: The following FCS_COP.1 SFRs are realized through MetaSIGN-API usage.

FCS_COP.1.1/Hash The TSF shall perform

[assignment]

o **hash generation** in accordance with a specified cryptographic algorithm **[assignment: hash algorithm] SHA-256, SHA-384 or SHA-512** and cryptographic key sizes **[assignment: hash size] none** that meet the following: **CRYPT-STD [assignment: list of standards] , FIPS 180-2.**

6.1.2.6 Identification et authentification de l'utilisateur

FMT_SMR.1/Verifier security roles

FMT_SMR.1.1/The TSF shall maintain the roles

[assignment]

- o **verifier**
- o **administrator. (assumed by using application)**

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

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

FIA_UID.2/Verification User identification before any action

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

Note d'application

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

6.2 Exigences de d'assurance de sécurité pour la TOE

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

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

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

Toutes les exigences d'assurance pour la TOE sont extraites de la partie 3 des Critères Communs [CC].

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

7 Argumentaires

7.1 Objectifs de sécurité / problème de sécurité

Seulun objectif de sécurité sur l'environnement a été ajouté de la manière suivante :

Objectifs de sécurité :	Type de modification :
OE.TOE.MVS.Tiers_De_Confiance_Sûr	Ajout

Compte tenu du fait que ces objectifs modifiés (ajoutés ou supprimés) ne portent que sur l'environnement de la TOE, ces modifications n'impactent pas les exigences fonctionnelles de sécurité de la TOE. Par conséquent, les argumentaires des profils de protection ([PP-ACSE-CCv3.1], [PP-MVSE-CCv3.1]) restent inchangés et s'appliquent ici.

7.1.1 Politiques de sécurité organisationnelles (OSP)

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

P.TOE.Conformité_Certificat_Signataire La politique de sécurité organisationnelle P.TOE. **Conformité_Certificat_Signataire** est couverte par les objectifs de sécurité sur la TOE :

- O.Conformité_Des_Certificats qui requière que la TOE vérifie que les certificats du chemin de certification (incluant le certificat du signataire) répondent bien aux critères de la politique de signature appliquée.
- O.Conformité_Du_Certificat qui requiert que la TOE contrôle que le certificat sélectionné par le signataire répond bien aux critères de la politique de signature à appliquer.

P.TOE.Validité_Certificat_Signataire La politique de sécurité organisationnelle P.TOE.Validité_Certificat_Signataire est couverte par les objectifs de sécurité sur la TOE:

- O.Référence_De_Temps qui requiert que la signature soit positionnée dans le temps. Cette couverture n'est applicable que dans le cas de signatures horodatées (CAdES-T, CAdES-C, CAdES-XL, CAdES-A, XAdES-T, XAdES-C, XAdES-XL, XAdES-A, PAdES-T, PAdES-LTV).
- O.Validité_Des_Certificats qui requiert que la TOE vérifie que le certificat du signataire utilisé pour la signature était bien valide au moment où la signature a été positionnée dans le temps.
- O.Validité_Du_Certificat qui requiert que la TOE contrôle la conformité du certificat sélectionné par le signataire est bien utilisé durant sa période de validité..

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

P.TOE.Conformité_Attributs_Signature La politique de sécurité organisationnelle P.TOE.Conformité_Attributs_Signature est complètement couverte par les objectifs de sécurité sur la TOE :

- O.Conformité_Attributs_Signés qui requière que la TOE vérifie la présence et la conformité des attributs signés en regard de la politique de signature.
- O.Conformité_Des_Attributs en requérant que la TOE contrôle la présence et la conformité de tous les attributs de signature requis par la politique de signature.

P.MVS.Authenticité_Certificat_Signataire La politique de sécurité organisationnelle P.MVS.Authenticité_Certificat_Signataire est couverte par l'objectif de sécurité sur la TOE O.Chemin_De_Certification qui requiert que la TOE contrôle qu'un chemin de certification valide existe pour attester l'authenticité du certificat du signataire utilisé pour la signature.

P.MVS.Authenticité/Intégrité_Données_Validation La politique de sécurité organisationnelle P.MVS.Authenticité/Intégrité_Données_De_Validation est couverte par l'objectif de sécurité O.Conformité_Données_Validation qui requiert notamment que ces données soient signées par leur émetteur.

7.1.1.2 Contrôle de l'invariance de la sémantique du document

P.TOE.Sémantique_Document_Invariante La politique de sécurité organisationnelle P.TOE.Sémantique_Document_Invariante est couverte d'une part, par les objectifs de sécurité sur la TOE:

- O.Contrôle_Invariance_Document qui requiert que la TOE interroge un module externe chargé de contrôler l'invariance de la sémantique du document signé, et définit les deux comportements alternatifs conformes à ceux définis dans cette politique;
- O.Invocation_Module_Controle_Invariance qui requiert que la TOE interroge un module externe chargé de contrôler l'invariance de la sémantique du document signé et communique le résultat du contrôle au vérificateur, d'autre part par l'objectif de sécurité sur l'environnement.

Et d'autre part, par l'objectif de sécurité sur l'environnement :

- OE.TOE.Contrôle_Sémantique_Document_Signer qui assure que l'environnement de la TOE fournit un module capable de déterminer l'invariance sémantique du document signé.

7.1.1.3 Présentation du document et des attributs de signature au signataire

P.TOE.Possibilité_De_Présenter_Le_Document La politique de sécurité est couverte par les objectifs O.Lancement_d'Applications_De_Présentation et OE.TOE.Présentation_Document qui requierent:

- d'une part que la TOE puisse lancer une application de visualisation externe en s'appuyant sur le format du document à signer,

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

- d'autre part que la TOE empêche la signature de documents pour lesquels une application de visualisation ne peut être lancée.

P.MCS.Présentation_Attributs_De_Signature Cette politique est couverte totalement par les objectifs de sécurité :
- O.Présentation_Conforme_Des_Attributs qui requiert que la TOE offre au signataire une représentation des attributs de signature conforme à ceux qui seront signés.
- O.Communication_Attributs_Signés qui exige que la TOE présente les attributs signés au Vérificateur.

7.1.1.4 Conformité aux standards

P.TOE.Algorithmes_De_Hachage La politique de sécurité organisationnelle P.TOE.Algorithme_De_Hachage est directement couverte par l'objectif de sécurité : O.Support_Cryptographique qui, sur ce point, en reprend les éléments.

P.MVS.Algorithmes_De_Signature La politique de sécurité organisationnelle P.MVS.Algorithmes_De_Signature est directement couverte par l'objectif de sécurité O.Support_Cryptographique qui, sur ce point, en reprend tous les éléments.

7.1.1.5 Interaction avec l'utilisateur (signataire ou vérificateur)

P.MCS.Signature_De_Plusieurs_Document La politique est couverte par l'objectif O.Ensemble_De_Documents_A_Signer qui demande que:
- la TOE garantisse que les documents signés soient ceux sélectionnés par le signataire (pas d'ajout de document, pas de suppression de document, pas de substitution de documents dans la liste);
- que des attributs de signature identiques soient utilisés lorsque le consentement du signataire porte sur un ensemble de plusieurs documents.

P.MCS.Arrêt_Processus_Signature Cette politique est couverte par l'objectif O.Abandon_Du_Processus_De_Signature en requérant que la TOE fournisse les moyens d'interrompre le processus de signature à tout moment avant l'activation de la clé privée de signature.

P.MCS.Consentement_Explicite Cette politique de sécurité organisationnelle est couverte par l'objectif O.Consentement_Explicite. Cet objectif oblige le signataire à exprimer sans ambiguïté sa volonté de signer. De cette manière la TOE oblige à exprimer de manière explicite son consentement à signer.

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

7.1.1.6 Contraintes diverses liées à la création de signature

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

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

7.1.1.7 Contraintes diverses liées à la vérification de signature

P.MVS.Export_Données_Validation Cette politique est couverte par l'objectif O.Export_Données_Validation qui reprend tous les éléments de celle-ci.

7.1.1.8 Contraintes diverses liées à l'administration

P.TOE.Administration Cette politique est couverte par l'objectif O.Administration qui requière que la TOE permette à l'administrateur de sécurité (assuré par l'application utilisatrice) de gérer (ajouter/supprimer) les politiques de signature et la table de correspondance entre les applications de visualisation et les formats de documents en entrée de la TOE et d'autre part par l'objectif de sécurité sur l'environnement OE.TOE.Administrateur_De_Sécurité qui assure que l'administrateur de sécurité (assuré par l'application utilisatrice de la TOE) n'est pas un agent menaçant.

7.1.2 Hypothèses

7.1.2.1 Hypothèses sur la machine hôte

H.Machine_Hôte L'hypothèse H.Machine_Hôte est couverte par l'objectif de sécurité sur l'environnement OE.TOE.Machine_Hôte qui en reprend les éléments.

7.1.2.2 Création de signature – Hypothèses relatives au dispositif de création de signature

H.MCS.Dispositif_De_Création_De_Signature L'hypothèse est couverte complètement par l'objectif OE.MCS.Dispositif_De_Création_De_Signature qui reprend tous les éléments de cette hypothèse.

H.MCS.Communication_TOE/SCDev Cette hypothèse est couverte entièrement par l'objectif OE.MCS.Communication_TOE/SCDev qui en reprend tous les éléments.

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

H.MCS.Authentification_Signataire Cette hypothèse est couverte entièrement par l'objectif OE.MCS.Protection_Données_Authentification_Signataire qui en reprend tous les éléments.

7.1.2.3 Présentation du document

H.MCS.Présentation_Du_Document Cette hypothèse est couverte en totalité par l'objectif OE.TOE.Présentation_Document qui reprend tous les éléments de celle-ci.

7.1.2.4 Hypothèse concernant l'invariance de la sémantique du document

H.MCS.Contrôle_Invariance_Sémantique_Document L'hypothèse H.Contrôle_Invariance_Sémantique_Document est couverte par l'objectif de sécurité sur l'environnement OE.Contrôle_Sémantique_Document_Signer qui en reprend les éléments.

7.1.2.5 Hypothèses sur le contexte d'utilisation

H.TOE.Politique_Signature_D'Origine_Authentique L'hypothèse H.TOE.Politique_De_Signature_D'Origine_Authentique est couverte par l'objectif de sécurité sur l'environnement OE.TOE.Authenticité_Origine_Politique_Signature demandant aux administrateurs (assuré par l'application utilisatrice de la TOE) de s'assurer de l'authenticité de l'origine des politiques de signature utilisables par la TOE.

H.MCS.Présence_Du_Signataire L'hypothèse H.MCS.Présence_Du_Signataire est complètement couverte par l'objectif de sécurité sur l'environnement OE.Présence_Du_Signataire qui en reprend les éléments.

H.MVS.Accès_Données_De_Validation L'hypothèse de sécurité organisationnelle H.MVS.Accès_Données_De_Validation est couverte par l'objectif sur l'environnement OE.MVS.Fourniture_Des_Données_De_Validation qui requiert que ce dernier fournisse les données de validation nécessaires à la vérification de la signature.

H.Administrateur_De_Sécurité_Sûr L'hypothèse H.Administrateur_De_Sécurité_Sûr est couverte entièrement par l'objectif sur l'environnement OE.Administrateur_De_Sécurité_Sûr qui en reprend les termes.

H.MCS.Intégrité_Services L'hypothèse H.MCS.Intégrité_Services est couverte entièrement par l'objectif sur l'environnement OE.TOE.Intégrité_Services qui en reprend les termes.
H.MVS.Tiers_De_Confiance_Sûr L'hypothèse H.MVS.Tiers_De_Confiance_Sûr est couverte entièrement par l'objectif sur l'environnement OE.TOE.MVS.Tiers_De_Confiance_Sûr qui en reprend les termes.

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

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

Politiques de sécurité organisationnelles (OSP)	**Objectifs de sécurité**	**Argumentaire**
P.TOE.Conformité_Certificat_Signataire	O.Conformité_Des_Certificats O.Conformité_Du_Certificat	Section 7.1.1.1
P.TOE.Validité_Certificat_Signataire	O.Référence_De_Temps O.Validité_Des_Certificats O.Validité_Du_Certificat	Section 7.1.1.1
P.TOE.Conformité_Attributs_Signature	O.Conformité_Attributs_Signés O.Conformité_Des_Attributs	Section 7.1.1.1
P.MVS.Authenticité_Certificat_Signataire	O.Chemin_De_Certification	Section 7.1.1.1
P.MVS.Authenticité/Intégrité_Données_Validation	O.Conformité_Données_Validation	Section 7.1.1.1
P.TOE.Sémantique_Document_Invariante	O.Contrôle_Invariance_Document O.Invocation_Module_Controle_Invariance OE.TOE.Contrôle_Sémantique_Document_Signer	Section 7.1.1.2
P.TOE.Possibilité_De_Présenter_Le_Document	O.Lancement_d'Applications_De_Présentation OE.TOE.Présentation_Document	Section 7.1.1.3
P.MCS.Présentation_Attributs_De_Signature	O.Présentation_Conforme_Des_Attributs O.Communication_Attributs_Signés	Section 7.1.1.3
P.TOE.Algorithmes_De_Hachage	O.Support_Cryptographique	Section 7.1.1.4
P.MVS.Algorithmes_De_Signature	O.Support_Cryptographique	Section 7.1.1.4
P.MCS.Signature_De_Plusieurs_Document	O.Ensemble_De_Documents_A_Signer	Section 7.1.1.5
P.MCS.Arrêt_Processus_Signature	O.Abandon_Du_Processus_De_Signature	Section 7.1.1.5
P.MCS.Consentement_Explicite	O.Consentement_Explicite	Section 7.1.1.5
P.MCS.Association_Certificat/Clé_privée	O.MCS.Association_Certificat/Clé_privée	Section 7.1.1.6
P.MCS.Export_Signature_Électronique	O.Export_Signature_Électronique	Section 7.1.1.6

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

P.MVS.Export_Données_Validation	O.Export_Données_Validation	Section 7.1.1.7
P.TOE.Administration	O.Administration OE.Administrateur_De_Sécurité_Sûr	Section 7.1.1.8

Tableau 1: Association politiques de sécurités organisationnelles vers objectifs de sécurité

Objectifs de sécurité	**Politiques de sécurité organisationnelles (OSP)**
O.Administration	P.TOE.Administration
O.Référence_De_Temps	P.TOE.Validité_Certificat_Signataire
O.Validité_Des_Certificats	P.TOE.Validité_Certificat_Signataire
O.Validité_Du_Certificat	P.TOE.Validité_Certificat_Signataire
O.Conformité_Des_Attributs	P.TOE.Conformité_Attributs_Signature
O.Conformité_Attributs_Signés	P.TOE.Conformité_Attributs_Signature
O.Conformité_Des_Certificats	P.TOE.Conformité_Certificat_Signataire
O.Conformité_Du_Certificat	P.TOE.Conformité_Certificat_Signataire
O.Chemin_De_Certification	P.MVS.Authenticité_Certificat_Signataire
O.Conformité_Données_Validation	P.MVS.Authenticité/Intégrité_Données_Validation
O.Contrôle_Invariance_Document	P.TOE.Sémantique_Document_Invariante
O.Invocation_Module_Controle_Invariance	P.TOE.Sémantique_Document_Invariante
O.Lancement_d'Applications_De_Présentation	P.TOE.Possibilité_De_Présenter_Le_Document
OE.TOE.Présentation_Document	P.TOE.Possibilité_De_Présenter_Le_Document
O.Présentation_Conforme_Des_Attributs	P.MCS.Présentation_Attributs_De_Signature
O.Support_Cryptographique	P.TOE.Algorithmes_De_Hachage P.MVS.Algorithmes_De_Signature
O.Ensemble_De_Documents_A_Signer	P.MCS.Signature_De_Plusieurs_Document

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

O.Abandon_Du_Processus_De_Signature	P.MCS.Arrêt_Processus_Signature
O.Consentement_Explicite	P.MCS.Consentement_Explicite
O.MCS.Association_Certificat/Clé_privée	P.MCS.Association_Certificat/Clé_privée
O.Export_Signature_Électronique	P.MCS.Export_Signature_Électronique
O.Export_Données_Validation	P.MVS.Export_Données_Validation
OE.Administrateur_De_Sécurité_Sûr	P.TOE.Administration
OE.TOE.Machine_Hôte	
OE.TOE.Authenticité_Origine_Politique_Signature	
OE.MVS.Fourniture_Des_Données_De_Validation	
OE.TOE. Application_Appelante_Sûre	
OE.MCS.Dispositif_De_Création_De_Signature	
OE.MCS.Communication_TOE/SCDev	
OE.MCS.Protection_Données_Authentification_Signataire	
OE.Présence_Du_Signataire	
OE.TOE.Contrôle_Sémantique_Document_Signer	P.TOE.Sémantique_Document_Invariante
OE.TOE.Intégrité_Services	
OE.TOE.MVS.Tiers_De_Confiance_Sûr	

Tableau 2 : Association objectifs de sécurité vers politiques de sécurité organisationnelles

Hypothèses	**Objectifs de sécurité pour l'environnement opérationnel**	**Argumentaire**
H.Machine_Hôte	OE.TOE.Machine_Hôte	Section 7.1.2.1
H.MCS.Dispositif_De_Création_De_Signature	OE.MCS.Dispositif_De_Création_De_Signature	Section 7.1.2.2
H.MCS.Communication_TOE/SCDev	OE.MCS.Communication_TOE/SCDev	Section 7.1.2.2
H.MCS.Authentification_Signataire	OE.MCS.Protection_Données_Authentification_Signataire	Section 7.1.2.2
H.MCS.Présentation_Du_Document	OE.TOE.Présentation_Document	Section 7.1.2.3

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

H.Contrôle_Invariance_Sémantique_Document	OE.Contrôle_Sémantique_Document_Signer	Section 7.1.2.4
H.TOE.Politique_Signature_D'Origine_Authentique	OE.TOE.Authenticité_Origine_Politique_Signature	Section 7.1.2.5
H.MCS.Présence_Du_Signataire	OE.Présence_Du_Signataire	Section 7.1.2.5
H.MVS.Accès_Données_De_Validation	OE.MVS.Fourniture_Des_Données_De_Validation	Section 7.1.2.5
H.Administrateur_De_Sécurité_Sûr	OE.Administrateur_De_Sécurité_Sûr	Section 7.1.2.5
H.MCS.Intégrité_Services	OE.TOE.Intégrité_Services	Section 7.1.2.5
H.MVS.Tiers_De_Confiance_Sûr	OE.TOE. MVS.Tiers_De_Confiance_Sûr	Section 7.1.2.5

Tableau 3 : Association hypothèses vers objectifs de sécurité pour l'environnement opérationnel

Objectifs de sécurité	**Politiques de sécurité organisationnelles (OSP)**
OE.TOE.Machine_Hôte	H.Machine_Hôte
OE.MCS.Dispositif_De_Création_De_Signature	H.MCS.Dispositif_De_Création_De_Signature
OE.MCS.Communication_TOE/SCDev	H.MCS.Communication_TOE/SCDev
OE.MCS.Protection_Données_Authentification_Signataire	H.MCS.Authentification_Signataire
OE.TOE.Présentation_Document	H.MCS.Présentation_Du_Document
OE.Contrôle_Sémantique_Document_Signer	H.Contrôle_Invariance_Sémantique_Document
OE.TOE.Authenticité_Origine_Politique_Signature	H.TOE.Politique_Signature_D'Origine_Authentique
OE.MVS.Fourniture_Des_Données_De_Validation	H.MVS.Accès_Données_De_Validation
OE.Administrateur_De_Sécurité_Sûr	H.Administrateur_De_Sécurité_Sûr
OE.Présence_Du_Signataire	H.MCS.Présence_Du_Signataire
OE.TOE.Intégrité_Services	H.MCS.Intégrité_Services
OE.TOE.MVS.Tiers_De_Confiance_Sûr	H.MVS.Tiers_De_Confiance_Sûr

Tableau 4 : Association objectifs de sécurité pour l'environnement opérationnel vers hypothèses

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

7.2 Exigences de sécurité / Objectifs de sécurité

7.2.1 Objectifs de sécurité pour la TOE

7.2.1.1 Objectifs de sécurités communs à MCS et MVS

O.Administration L'objectif O.Administration est couvert par les composants fonctionnels suivants:

- FMT_SMR.1/Signer security roles et FMT_SMR.1/Verifier security roles qui requiert que la TOE différencie le rôle de l'administrateur (assuré par l'application utilisatrice) de la TOE du rôle de signataire ou de vérificateur;
- FMT_MTD.1/Document format/viewer association table Management, FMT_SMF.1/Management of the document format/viewer association table for signature et FMT_SMF.1/Management of the document format/viewer association table for verifying qui permettent à l'administrateur (assuré par l'application utilisatrice de la TOE) (et uniquement lui) de modifier la table d'association entre les formats de documents et les programmes de visualisation;
- FMT_SMF.1/Management of the signature policies qui définissent les opérations de gestion applicables aux politiques de signature et FMT_MTD.1/Management of the signature policies qui restreint leur utilisation au seul administrateur (assuré par l'application utilisatrice de la TOE).
- FMT_SMF.1/Management of the viewer activation parameter qui définit la fonction permettant d'inhiber la fonction de visualisation du document signé

7.2.1.2 Présentation du ou des documents à signer ou signés

O.Lancement_d'Applications_De_Présentation L'objectif de sécurité O.Lancement_d'Applications_De_Présentation est couvert par les composants d'exigence suivants:

- FDP_IFF.1/Signature generation et FDP_IFF.1/Electronic signature, qui assure que l'utilisateur pourra visualiser le document à travers une application de visualisation externe. La TOE lance automatiquement l'application de visualisation associée au format du document à signer en utilisant une liste d'associations format document/visualisateur.
- FMT_MTD.1/Document format/viewer association table Management, FMT_SMF.1/Management of the document format/viewer association table for signature et FMT_SMF.1/Management of the document format/viewer association table for verifying garantissent que le contenu de la liste d'associations format document/visualisateur ne peut être modifiée que par un administrateur (assuré par l'application utilisatrice) de la TOE.
- FMT_MTD.1/Viewer activation parameter et FMT_SMF.1/Management of the viewer activation parameter qui garantissent que le paramètre d'activation de la fonction de

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

visualisation du document signé ne peut être modifiée que par un administrateur (assuré par l'application utilisatrice) de la TOE.

7.2.1.3 Objectifs de sécurité pour le Module de Création de Signature (MCS)

Objectifs généraux

O.Association_Certificat/Clé_privée L'objectif O.Association_Certificat/Clé_privée est couvert par l'exigence FDP_IFF.1/Signature generation. Cette exigence requiert que la TOE soit capable d'activer la clé privée de signature correspondant au certificat sélectionné par le signataire.

Interaction avec le signataire

O.Présentation_Conforme_Des_Attributs L'objectif O.Présentation_Conforme_Des_Attributs est couvert par l'exigence fonctionnelle FDP_IFF.1/Signature generation qui requiert notamment que la TOE puisse présenter les attributs de signature au signataire avant le début du processus de signature.

O.Consentement_Explicite L'objectif O.Consentement_Explicite est couvert par l'exigence FDP_ITC.1/Explicit signer agreement par laquelle la TOE impose qu'une suite d'opérations non triviales soit réalisée avant de considérer la volonté de signer comme effective.

O.Abandon_Du_Processus_De_Signature L'objectif O.Abandon_Du_Processus_De_Signature est couvert par le composant d'exigence FDP_ROL.2/Abort of the signature process qui assure que le signataire a la possibilité d'annuler la signature avant l'envoi des données au SCDev.

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

- FMT_MSA.1/Signature attributes qui restreint a seule l'application utilisatrice de la TOE la capacité de sélectionner les attributs de signature.
- FMT_SMF.1/Modification of signature attributes qui requiert que la TOE offre la possibilité de modifier la valeur des attributs de signature tant que le signataire n'a pas donné son agrément à signer.

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

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

Application d'une politique de signature

O.Conformité_Du_Certificat L'objectif de sécurité O.Conformité_Du_Certificat est couvert de la manière suivante:
La TOE doit appliquer une politique de contrôle de flux d'informations lors de l'import d'un certificat (FDP_IFC.1/Signer's certificate import). Le composant fonctionnel FDP_IFF.1/Signer's certificate import définit que cette politique de contrôle de flux permettra effectivement l'import du certificat dans la TOE si des règles définies dans la politique de signature sont bien remplies. Ces règles portent sur le certificat du signataire.
La conformité du certificat sélectionné est garantie si les attributs de celui-ci remplissent le sous-ensemble de règles défini dans la politique de signature.
Les composants fonctionnels FDP_ITC.2/Signer's certificate et FPT_TDC.1/Signer's certificate assurent d'une part que la TOE applique les règles de la politique de contrôle de flux lors de l'import du certificat sélectionné et d'autre part que la TOE est en mesure d'exploiter les données contenues dans le certificat importé.
Les composants fonctionnels suivants, portant sur la gestion des attributs de sécurité des sujets et informations mis en jeu dans la politique de contrôle de flux contribuent eux aussi à couvrir cet objectif:

- Le composant fonctionnel FMT_MSA.3/Signer's certificate import garantit que les valeurs par défaut attribuées aux attributs de sécurité mis en jeu dans la politique de contrôle de flux prennent des valeurs restrictives.
- Les composants fonctionnels FMT_MSA.1/Signer's certificate et FMT_SMF.1/Signer's certificate selection garantissent au signataire le droit exclusif de sélectionner le certificat approprié pour une signature électronique qu'il souhaite réaliser.
- Le composant FMT_SMR.1/Signer security roles demande à la TOE de différencier le rôle de signataire du rôle de d'administrateur (assuré par l'application utilisatrice) de la TOE.
- Le composant FIA_UID.2/Signature User identification before any action requiert que la TOE ne permette la réalisation d'aucune opération avant d'avoir identifié avec succès l'utilisateur.

O.Validité_Du_Certificat L'objectif de sécurité O.Validité_Du_Certificat est couvert de la manière suivante:
La TOE doit appliquer une politique de contrôle de flux d'informations lors de l'import d'un certificat (FDP_IFC.1/Signer's certificate import). Le composant fonctionnel FDP_IFF.1/Signer's certificate import définit que cette politique de contrôle de flux permettra effectivement l'import du certificat dans la TOE si des règles définies dans la politique de signature sont bien remplies. Ces règles portent sur le certificat du signataire.
La conformité du certificat sélectionné est garantie si les attributs de celui-ci remplissent le sous-ensemble de règles défini dans la politique de signature.
Les composants fonctionnels FDP_ITC.2/Signer's certificate et FPT_TDC.1/Signer's certificate assurent d'une part que la TOE applique les règles de la politique de contrôle de flux lors de l'import du certificat sélectionné et d'autre part que la TOE est en mesure d'exploiter les données contenues dans le certificat importé.

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

Les composants fonctionnels suivants, portant sur la gestion des attributs de sécurité des sujets et informations mis en jeu dans la politique de contrôle de flux contribuent eux aussi à couvrir cet objectif:

- Le composant fonctionnel FMT_MSA.3/Signer's certificate import garantit que les valeurs par défaut attribuées aux attributs de sécurité mis en jeu dans la politique de contrôle de flux prennent des valeurs restrictives.
- Les composants fonctionnels FMT_MSA.1/Signer's certificate et FMT_SMF.1/Signer's certificate selection garantissent au signataire le droit exclusif de sélectionner le certificat approprié pour une signature électronique qu'il souhaite réaliser.
- Le composant FMT_SMR.1/Signer security roles demande à la TOE de différencier le rôle de signataire du rôle d'administrateur (assuré par l'application utilisatrice) de la TOE.
- Le composant FIA_UID.2/Signature User identification before any action requiert que la TOE ne permette la réalisation d'aucune opération avant d'avoir identifié avec succès l'utilisateur.

O.Conformité_Des_Attributs L'objectif de sécurité O.Conformité_Des_Attributs est couvert de la manière suivante:
La TOE doit appliquer une politique de contrôle de flux d'informations lors de la génération d'une signature (FDP_IFC.1/Signature generation). Le composant fonctionnel FDP_IFF.1/Signature generation définit que cette politique de contrôle de flux permettra la génération de la signature (c'est-à-dire l'envoi des données à signer formatées au SCDev) si des règles définies dans la politique de signature sont bien remplies. Ce dernier composant comprend également des règles relatives aux attributs de la signature. La conformité des attributs de signature est garantie si ces attributs remplissent le sous ensemble de règles défini dans la politique de signature.
Les composants fonctionnels suivants, portant sur la gestion des attributs de sécurité des sujets et informations mis en jeu dans la politique de contrôle de flux contribuent eux aussi à couvrir cet objectif:

- Le composant fonctionnel FMT_MSA.3/Signature generation garantit que les valeurs par défaut attribuées aux attributs de sécurité mis en jeu dans la politique de contrôle de flux prennent des valeurs restrictives.
- Le composant fonctionnel FMT_MSA.1/Signature attributes et FMT_SMF.1/Modification of signature attributes garantit au signataire le droit exclusif de sélectionner le certificat approprié pour une signature électronique qu'il souhaite réaliser.
- Le composant FMT_SMR.1/Signer security roles demande à la TOE de différencier le rôle de signataire du rôle d'administrateur (assuré par l'application utilisatrice) de la TOE.
- Le composant FIA_UID.2/Signature User identification before any action requiert que la TOE ne permette la réalisation d'aucune opération avant d'avoir identifié avec succès l'utilisateur.

O.Export_Signature_Électronique L'objectif de sécurité O.Export_Signature_Électronique est couvert de la manière suivante:
La TOE doit appliquer une politique de contrôle de flux d'informations lors de l'import d'un document dans le champ de contrôle de la TOE (FDP_IFC.1/Electronic signature export). Le composant fonctionnel FDP_IFF.1/Electronic signature export définit les règles à appliquer par la TOE pour accepter de retourner la signature électronique.

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

Le composant FDP_ETC.2/Electronic signature export requiert que la TOE invoque un module externe pour déterminer si la sémantique du document est stable ou non, au moment où elle importe le document.
Les composants fonctionnels suivants, portant sur la gestion des attributs de sécurité des sujets et informations mis en jeu dans la politique de contrôle de flux contribuent eux aussi à couvrir cet objectif:

- Le composant fonctionnel FMT_MSA.3/Electronic signature export garantit que les valeurs par défaut attribuées aux attributs de sécurité mis en jeu dans la politique de contrôle de flux prennent des valeurs restrictives.
- Le composant fonctionnel FMT_SMF.1/Getting SCDev's signature generation status requiert que la TOE soit capable de recevoir du SCDev le statut de l'opération de génération de la signature numérique.
- Le composant fonctionnel FMT_MSA.1/SCDev signature generation status qui ne permet à personne de modifier le statut de l'opération de génération de la signature retourné par le SCDev.
- Le composant FMT_SMR.1/Signer security roles demande à la TOE de différencier le rôle de signataire du rôle de l'administrateur (assuré par l'application utilisatrice) de la TOE.
- Le composant FIA_UID.2/Signature User identification before any action requiert que la TOE ne permette la réalisation d'aucune opération avant d'avoir identifié avec succès l'utilisateur.

Contrôle de l'invariance de la sémantique du document

O.Contrôle_Invariance_Document L'objectif de sécurité O.Contrôle_Invariance_Sémantique_Du_Document est couvert de la manière suivante:
La TOE doit appliquer une politique de contrôle de flux d'informations lors de l'import d'un document dans le champ de contrôle de la TOE (FDP_IFC.1/Document acceptance for signature et FDP_IFC.1/Document acceptance for verifiyng). Le composant fonctionnel FDP_IFF.1/Document acceptance for signature définit les règles à appliquer par la TOE pour accepter le document à signer. Le composant fonctionnel FDP_IFF.1/Document acceptance for verifying définit les règles à appliquer par la TOE pour accepter le document signé à vérifier.
Les composants FDP_ITC.1/Document acceptance for signature et FDP_ITC.1/Document acceptance for verifying requierent que la TOE invoque un module externe pour déterminer si la sémantique du document est stable ou non, au moment où elle importe le document.
Les composants fonctionnels suivants, portant sur la gestion des attributs de sécurité des sujets et informations mis en jeu dans la politique de contrôle de flux contribuent eux aussi à couvrir cet objectif:

- Les composants fonctionnels FMT_MSA.3/Document's acceptance for signature et FMT_MSA.3/Document's acceptance for verifying garantissent que les valeurs par défaut attribuées aux attributs de sécurité mis en jeu dans la politique de contrôle de flux prennent des valeurs restrictives.
- Les composants fonctionnels FMT_MSA.1/Document's semantics invariance status for signature, FMT_MSA.1/Document's semantics invariance status for verifying,

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

FMT_SMF.1/Getting document's semantics invariance status for signature et FMT_SMF.1/Getting document's semantics invariance status qui requièrent for verifying d'une part que la TOE dispose d'un moyen d'invoquer un module externe pour obtenir le statut définissant si la sémantique du document est stable, d'autre part que personne ne puisse modifier ce statut une fois obtenu.

- Les composants fonctionnels FMT_MSA.1/Signer agreement to sign an instable document et FMT_SMF.1/Getting signer agreement to sign an instable document garantissent que seul le signataire peut modifier l'attribut permettant à la TOE de continuer le processus de signature d'un document dont la sémantique n'est pas déterminée comme stable.
- Le composant FMT_SMR.1/Signer security roles demande à la TOE de différencier le rôle de signataire du rôle d'administrateur (assuré par l'application utilisatrice) de la TOE.
- Le composant FIA_UID.2/Signature User identification before any action requiert que la TOE ne permette la réalisation d'aucune opération avant d'avoir identifié avec succès l'utilisateur.

7.2.1.4 Objectifs pour le Module de Vérification de Signature (MVS)

Objectifs sur les règles de verification

O.Référence_De_Temps L'objectif de sécurité O.Référence_De_Temps est couvert de la manière suivante:
La TOE doit appliquer une politique de contrôle de flux d'informations (FDP_IFC.1/Time reference) lors de l'import de la référence de temps associée à la signature numérique pour accepter cette référence comme valide. Le composant fonctionnel FDP_IFF.1/Time reference définit les règles à appliquer sur les différentes données mises en jeu pour déterminer si la référence de temps est valide; certaines règles portent sur la référence de temps elle-même, d'autres portent sur les données de validation de cette référence. Ce composant liste en plus l'ensemble de règles applicables aux données de validation sont définies au sein du composant fonctionnel; selon la politique de signature appliquée, un sous-ensemble de ces règles sera effectivement appliqué.
Les composants fonctionnels FMT_MTD.1/Selection of the applied signature policy et FMT_SMF.1/Selection of the applied signature policy définissent que seul le vérificateur (assuré par l'application utilisatrice) de la TOE peut sélectionner la politique de signature à appliquer.
Les composants fonctionnels FDP_ITC.2/Time reference et FPT_TDC.1/Time reference assurent d'une part que la TOE applique la politique de contrôle de flux lors de l'import de la référence de temps et d'autre part que la TOE est en mesure d'interpréter les données importées et donc de les exploiter.
Les composants fonctionnels suivants, portant sur la gestion des attributs de sécurité des sujets et informations mis en jeu dans la politique de contrôle de flux contribuent eux aussi à couvrir cet objectif:

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

- Le composant fonctionnel FMT_MSA.3/Time reference garantit que les valeurs par défaut attribuées aux attributs de sécurité mis en jeu dans la politique de contrôle de flux prennent des valeurs restrictives.
- Le composant fonctionnel FMT_MSA.1/Time reference garantit la non modification des attributs de sécurité de la référence de temps.
- Le composant fonctionnel FMT_MSA.1/Certificates garantit la non modification des attributs des certificats impliqués dans la vérification de la validité de la référence de temps.
- Le composant fonctionnel FMT_MSA.1/Certificates' validation data garantit la non modification des attributs des données de validation des certificats impliqués dans le contrôle de la validité de la référence de temps.
- Le composant FMT_SMR.1/Verifier security roles demande à la TOE de différencier le rôle de vérificateur du rôle de l'administrateur (assuré par l'application utilisatrice) de la TOE.
- Le composant FIA_UID.2/Verification User identification before any action requiert que la TOE ne permette la réalisation d'aucune opération avant d'avoir identifié avec succès l'utilisateur.

O.Chemin_De_Certification L'objectif de sécurité O.Chemin_De_Certification est couvert de la manière suivante:
La TOE doit appliquer une politique de contrôle de flux d'informations (FDP_IFC.1/Certification path) lors de l'import d'un ensemble de certificats constituant un chemin de certification entre le certificat du signataire et un certificat racine défini dans la politique de signature.
Le composant fonctionnel FDP_ITC.2/Certification path assure que la TOE applique la politique de contrôle de flux lors de l'import des certificats. Les composants FPT_TDC.1/Certificates et FPT_TDC.1/Certificate revocation data assurent que la TOE est bien en mesure d'exploiter ces données.
Les règles de la politique de contrôle de flux sont définies dans le composant fonctionnel FDP_IFF.1/Certification path. Ce composant définit l'ensemble des règles devant être implémentées.
Les règles à vérifier pour assurer la validité du chemin de certification sont définies par la politique de signature appliquée. Cette politique ne peut être choisie que par le vérificateur (assuré par l'application utilisatrice) de la TOE (FMT_MTD.1/Selection of the applied signature policy et FMT_SMF.1/Selection of the applied signature policy).
Les composants fonctionnels suivants, portant sur la gestion des attributs de sécurité des sujets et informations mis en jeu dans la politique de contrôle de flux contribuent eux aussi à couvrir cet objectif:

- Le composant fonctionnel FMT_MSA.3/Certification path garantit que les valeurs par défaut attribuées aux attributs de sécurité mis en jeu dans la politique de contrôle de flux prennent des valeurs restrictives.
- Le composant fonctionnel FMT_MSA.1/Certificates garantit la non modification des attributs des certificats importés pour construire le chemin de certification.
- Le composant fonctionnel FMT_MSA.1/Certificates' validation data garantit la non modification des attributs des données de validation du certificat du signataire.

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

Enfin les composants suivants contribuent à la bonne application de la politique de contrôle de flux:

- Le composant FMT_SMR.1/Verifier security roles demande à la TOE de différencier le rôle de vérificateur du rôle de l'administrateur (assuré par l'application utilisatrice) de la TOE.
- Le composant FIA_UID.2/Verification User identification before any action requiert que la TOE ne permette la réalisation d'aucune opération avant d'avoir identifié avec succès l'utilisateur.

O.Conformité_Des_Certificats L'objectif de sécurité O.Conformité_Des_Certificats est couvert de la manière suivante:
La TOE doit appliquer une politique de contrôle de flux d'informations (FDP_IFC.1/Certification path) lors de l'import d'un ensemble de certificats constituant un chemin de certification entre le certificat du signataire et un certificat racine défini dans la politique de signature.
Le composant fonctionnel FDP_ITC.2/Certification path assure que la TOE applique la politique de contrôle de flux lors de l'import des certificats. Les composants FPT_TDC.1/Certificates et FPT_TDC.1/Certificate revocation data assurent que la TOE est bien en mesure d'exploiter ces données.
Les règles de la politique de contrôle de flux sont définies dans le composant fonctionnel FDP_IFF.1/Certification path qui indique l'ensemble des règles devant être implémentées.
Les règles à vérifier pour assurer la validité du chemin de certification sont définies par la politique de signature appliquée. Cette politique ne peut être choisie que par le vérificateur (assuré par l'application utilisatrice) de la TOE (FMT_MTD.1/Selection of the applied signature policy et FMT_SMF.1/Selection of the applied signature policy).
Les composants fonctionnels suivants, portant sur la gestion des attributs de sécurité des sujets et informations mis en jeu dans la politique de contrôle de flux contribuent eux aussi à couvrir cet objectif:

- Le composant fonctionnel FMT_MSA.3/Certification path garantit que les valeurs par défaut attribuées aux attributs de sécurité mis en jeu dans la politique de contrôle de flux prennent des valeurs restrictives.
- Le composant fonctionnel FMT_MSA.1/Certificates garantit la non modification des attributs des certificats importés pour construire le chemin de certification.
- Le composant fonctionnel FMT_MSA.1/Certificates' validation data garantit la non modification des attributs des données de validation du certificat du signataire.

Enfin les composants suivants contribuent à la bonne application de la politique de contrôle de flux:

- Le composant FMT_SMR.1/Verifier security roles demande à la TOE de différencier le rôle de vérificateur du rôle de l'administrateur (assuré par l'application utilisatrice) de la TOE.
- Le composant FIA_UID.2/Verification User identification before any action requiert que la TOE ne permette la réalisation d'aucune opération avant d'avoir identifié avec succès l'utilisateur.

O.Validité_Des_Certificats L'objectif de sécurité O.Validité_Des_Certificats est couvert de la manière suivante:

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

La TOE doit appliquer une politique de contrôle de flux d'informations (FDP_IFC.1/Certification path) lors de l'import d'un ensemble de certificats constituant un chemin de certification entre le certificat du signataire et un certificat racine défini dans la politique de signature.
Le composant fonctionnel FDP_ITC.2/Certification path assure que la TOE applique la politique de contrôle de flux lors de l'import des certificats et des informations de non révocation.
Les composants FPT_TDC.1/Certificates et en particulier FPT_TDC.1/Certificate revocation data assurent que la TOE est bien en mesure d'exploiter ces données.
Les règles de la politique de contrôle de flux sont définies dans le composant fonctionnel FDP_IFF.1/Certification path. Ce composant indique l'ensemble des règles devant être implémentées. Cette exigence comportent notamment des règles permettant à la TSF de s'assurer que les certificats du chemin sont bien en cours de validité et que leur état est non révoqué.
Les règles à vérifier effectivement pour assurer la validité des certificats du chemin sont définies par la politique de signature appliquée. Cette politique ne peut être choisie que par le vérificateur (assuré par l'application utilisatrice) de la TOE (FMT_MTD.1/Selection of the applied signature policy et FMT_SMF.1/Selection of the applied signature policy).
Les composants fonctionnels suivants, portant sur la gestion des attributs de sécurité des sujets et informations mis en jeu dans la politique de contrôle de flux contribuent eux aussi à couvrir cet objectif:

- Le composant fonctionnel FMT_MSA.3/Certification path garantit que les valeurs par défaut attribuées aux attributs de sécurité mis en jeu dans la politique de contrôle de flux prennent des valeurs restrictives.
- Le composant fonctionnel FMT_MSA.1/Certificates garantit la non modification des attributs des certificats importés pour construire le chemin de certification.
- Le composant fonctionnel FMT_MSA.1/Certificates' validation data garantit la non modification des attributs des données de validation du certificat du signataire.

Enfin les composants suivants contribuent à la bonne application de la politique de contrôle de flux:

- Le composant FMT_SMR.1/Verifier security rolesdemande à la TOE de différencier le rôle de vérificateur du rôle de l'administrateur (assuré par l'application utilisatrice) de la TOE.
- Le composant FIA_UID.2/Verification User identification before any action requiert que la TOE ne permette la réalisation d'aucune opération avant d'avoir identifié avec succès l'utilisateur.

O.Conformité_Données_Validation L'objectif de sécurité O.Conformité_Données_Validation est couvert de la manière suivante:
La TOE doit appliquer une politique de contrôle de flux d'informations (FDP_IFC.1/Certification path) lors de l'import d'un ensemble de certificats constituant un chemin de certification entre le certificat du signataire et un certificat racine défini dans la politique de signature. Cette politique de contrôle de flux s'applique aussi aux informations de non-révocation associées aux certificats.
Le composant fonctionnel FDP_ITC.2/Certification path assure que la TOE applique la politique de contrôle de flux lors de l'import des certificats et des informations de non révocation.
Les composants FPT_TDC.1/Certificates et en particulier FPT_TDC.1/Certificate revocation data assurent que la TOE est bien en mesure d'exploiter ces données.
Les règles de la politique de contrôle de flux sont définies dans le composant fonctionnel FDP_IFF.1/Certification path. Ce dernier composant indique l'ensemble des règles devant être

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

implémentées et comporte des règles permettant à la TSF de s'assurer de la validité les données de révocation des certificats.
Les règles à vérifier pour assurer la validité des informations de révocation des certificats du chemin sont définies par la politique de signature appliquée. Cette politique ne peut être choisie que par le vérificateur (assuré par l'application utilisatrice) de la TOE (FMT_MTD.1/Selection of the applied signature policy et FMT_SMF.1/Selection of the applied signature policy).
Les composants fonctionnels suivants, portant sur la gestion des attributs de sécurité des sujets et informations mis en jeu dans la politique de contrôle de flux contribuent eux aussi à couvrir cet objectif:

- Le composant fonctionnel FMT_MSA.3/Certification path garantit que les valeurs par défaut attribuées aux attributs de sécurité mis en jeu dans la politique de contrôle de flux prennent des valeurs restrictives.
- Le composant fonctionnel FMT_MSA.1/Certificates garantit la non modification des attributs des certificats importés pour construire le chemin de certification.
- Le composant fonctionnel FMT_MSA.1/Certificates' validation data garantit la non modification des attributs des données de validation du certificat du signataire.

Enfin les composants suivants contribuent à la bonne application de la politique de contrôle de flux:

- Le composant FMT_SMR.1/Verifier security roles demande à la TOE de différencier le rôle de vérificateur du rôle de l'administrateur (assuré par l'application utilisatrice) de la TOE.
- Le composant FIA_UID.2/Verification User identification before any action requiert que la TOE ne permette la réalisation d'aucune opération avant d'avoir identifié avec succès l'utilisateur.

O.Conformité_Attributs_Signés L'objectif de sécurité O.Conformité_Attributs_Signés est couvert de la manière suivante:
La TOE doit appliquer une politique de contrôle de flux d'informations au moment de l'import de la signature électronique (FDP_IFC.1/Electronic signature validation). Le composant fonctionnel FDP_IFF.1/Electronic signature validation définit les règles à appliquer notamment pour contrôler la conformité des attributs signés vis-à-vis de la politique de signature. Ce dernier composant définit également l'ensemble des règles devant être implémentées par la TOE. La politique de signature appliquée invoque un sous ensemble de ces règles.
Les composants fonctionnels FMT_MTD.1/Selection of the applied signature policy et FMT_SMF.1/Selection of the applied signature policy définissent que seul le vérificateur (assuré par l'application) utilisatrice de la TOE peut sélectionner la politique de signature à appliquer.
Les composants fonctionnels FDP_ITC.2/Electronic signature et FPT_TDC.1/Electronic signature assurent d'une part que la TOE applique la politique de contrôle de flux lors de l'import de la signature électronique (comportant des attributs signés) et d'autre part que la TOE est bien en mesure d'interpréter et donc d'exploiter ces données.
Les composants fonctionnels suivants, portant sur la gestion des attributs de sécurité des sujets et informations mis en jeu dans la politique de contrôle de flux contribuent eux aussi à couvrir cet objectif:

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

- Le composant fonctionnel FMT_MSA.3/Electronic signature garantit que les valeurs par défaut attribuées aux attributs de sécurité mis en jeu dans la politique de contrôle de flux prennent des valeurs restrictives.
- Le composant fonctionnel FMT_MSA.1/Electronic signature garantit la non modification des attributs de la signature.

Enfin les composants suivants contribuent à la bonne application de la politique de contrôle de flux:

- Le composant FMT_SMR.1/Verifier security roles demande à la TOE de différencier le rôle de vérificateur du rôle de l'administrateur (assuré par l'application utilisatrice) de la TOE.
- Le composant FIA_UID.2/Verification User identification before any action requiert que la TOE ne permette la réalisation d'aucune opération avant d'avoir identifié avec succès l'utilisateur.

Objectifs relatifs à la visualisation des données signées

O.Communication_Attributs_Signés

L'objectif de sécurité est couvert par les composants d'exigence suivants:

- FDP_IFF.1/Electronic signature, qui requiert que la TOE soit capable d'exporter les attributs de la signature.

O.Export_Données_Validation

L'objectif de sécurité est couvert de la manière suivante:

La TOE doit appliquer une politique de contrôle de flux d'informations au moment d'exporter le résultat de la vérification de la signature (FDP_IFC.1/Electronic signature validation et FDP_IFF.1/Electronic signature validation).

Le composant fonctionnel FDP_ETC.2/Verification status requiert que le statut de vérification de la signature soit communiqué avec les données de validation prouvant son exactitude et avec les informations nécessaires au vérificateur pour traiter la signature (attributs signés, champs du certificat du signataire,...)

Les composants fonctionnels suivants, portant sur la gestion des attributs de sécurité des sujets et informations mis en jeu dans la politique de contrôle de flux contribuent eux aussi à couvrir cet objectif:

- Le composant fonctionnel FMT_MSA.3/Signature validation status garantit que les valeurs par défaut attribuées aux attributs de sécurité mis en jeu dans la politique de contrôle de flux prennent des valeurs restrictives.
- Le composant fonctionnel FMT_MSA.1/Signature validation status garantit la non modification du statut de la signature.

Enfin les composants suivants contribuent à la bonne application de la politique de contrôle de flux:

- Le composant FMT_SMR.1/Verifier security roles demande à la TOE de différencier le rôle de vérificateur du rôle d'administrateur (assuré par l'application utilisatrice) de la TOE.

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

- Le composant FIA_UID.2/Verification User identification before any action requiert que la TOE ne permette la réalisation d'aucune opération avant d'avoir identifié avec succès l'utilisateur.

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

O.Invocation_Module_Controle_Invariance L'objectif de sécurité O.Invocation_Module_Contrôle_Invariance est couvert de la manière suivante:
La TOE doit appliquer une politique de contrôle de flux d'informations lors de l'import d'un document dans le champ de contrôle de la TOE (FDP_IFC.1/Document acceptance for signature et FDP_IFC.1/Document acceptance for verifying). Le composant fonctionnel FDP_IFF.1/Document acceptance for signature définit les règles à appliquer par la TOE pour accepter le document à signer. Le composant fonctionnel FDP_IFF.1/Document acceptance for verifying définit les règles à appliquer par la TOE pour accepter le document signé à vérifier.
Les composants FDP_ITC.1/Document acceptance for signature et FDP_ITC.1/Document acceptance for verifying requierent que la TOE invoque un module externe pour déterminer si la sémantique du document est stable ou non, au moment où elle importe le document.
Les composants fonctionnels suivants, portant sur la gestion des attributs de sécurité des sujets et informations mis en jeu dans la politique de contrôle de flux contribuent eux aussi à couvrir cet objectif:

- Les composants fonctionnels FMT_MSA.3/Document's acceptance for signature et FMT_MSA.3/Document's acceptance for verifying garantissent que les valeurs par défaut attribuées aux attributs de sécurité mis en jeu dans la politique de contrôle de flux prennent des valeurs restrictives.
- Les composants fonctionnels FMT_MSA.1/Document's semantics invariance status for signature, FMT_MSA.1/Document's semantics invariance status for verifying, FMT_SMF.1/Getting document's semantics invariance status for signature et FMT_SMF.1/Getting document's semantics invariance status for verifying qui requièrent d'une part que la TOE dispose d'un moyen d'invoquer un module externe pour obtenir le statut définissant si la sémantique du document est stable, d'autre part que personne ne puisse modifier ce statut une fois obtenu.
- Le composant FMT_SMR.1/Verifier security roles demande à la TOE de différencier le rôle de signataire ou du vérificateur du rôle d'administrateur (assuré par l'application utilisatrice) de la TOE.
- Le composant FIA_UID.2/Verification User identification before any action requiert que la TOE ne permette la réalisation d'aucune opération avant d'avoir identifié avec succès l'utilisateur.

Conformité aux standards

O.Support_Cryptographique L'objectif de sécurité O.Support_Cryptographique est couvert par les exigences:

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

- FCS_COP.1/Hash Cryptographic operation pour ce qui concerne la propriété de non collision entre les condensés formatés produits par l'application de l'algorithme de hachage.
- FCS_COP.1/Signature verification qui garantit que tous les algorithmes cryptographiques utilisés dans le processus de vérification de la signature électronique sont résistants 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.

7.2.2 Tables de couverture entre objectifs et exigences de sécurité

Objectifs de sécurité	**Exigences fonctionnelles pour la TOE**	**Argumentaire**
O.Administration	FMT_SMR.1/Signer security roles, FMT_SMR.1/Verifier security roles FMT_MTD.1/Document format/viewer association table Management FMT_SMF.1/Management of the document format/viewer association table for signature FMT_SMF.1/Management of the document format/viewer association table for verifying FMT_MTD.1/Management of the signature policies FMT_SMF.1/Management of the signature policies	
O.Lancement_d'Applications_De_Présentation	FDP_IFF.1/Signature generation FDP_IFF.1/Electronic signature FMT_MTD.1/Document format/viewer association table Management FMT_SMF.1/Management of the document format/viewer association table for signature FMT_SMF.1/Management of the document format/viewer association table for verifying FMT_MTD.1/Viewer activation parameter	

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

	FMT_SMF.1/Management of the viewer activation parameter	
O.Association_Certificat/Clé_privée	FDP_IFF.1/Signature generation	Section 7.2.1.3
O.Présentation_Conforme_Des_Attributs	FDP_IFF.1/Signature generation	
O.Consentement_Explicite	FDP_ITC.1/Explicit signer agreement	Section 7.2.1.3
O.Abandon_Du_Processus_De_Signature	FDP_ROL.2/Abort of the signature process	Section 7.2.1.3
O.Ensemble_De_Documents_A_Signer	FMT_MSA.1/Selected documents FMT_SMF.1/Selection of a list of documents FMT_MSA.1/Signature attributes FMT_SMF.1/Modification of signature attributes	Section 7.2.1.3
O.Conformité_Du_Certificat	FDP_IFC.1/Signer's certificate import FDP_IFF.1/Signer's certificate import FDP_ITC.2/Signer's certificate FPT_TDC.1/Signer's certificat FMT_MSA.3/Signer's certificate import FMT_MSA.1/Signer's certificate FMT_SMF.1/Signer's certificate selection FMT_SMR.1/Signer security roles FIA_UID.2/Signature User identification before any action	Section 7.2.1.3
O.Validité_Du_Certificat	FDP_IFC.1/Signer's certificate import FDP_IFF.1/Signer's certificate import FDP_ITC.2/Signer's certificate FPT_TDC.1/Signer's certificate FMT_MSA.3/Signer's certificate import FMT_MSA.1/Signer's certificate FMT_SMF.1/Signer's certificate selection FMT_SMR.1/Signer security roles FIA_UID.2/Signature User identification before any action	Section 7.2.1.3

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

O.Conformité_Des_Attributs	FDP_IFC.1/Signature generation FDP_IFF.1/Signature generation FMT_MSA.3/Signature generation FMT_MSA.1/Signature attributes FMT_SMF.1/Modification of signature attributes FMT_SMR.1/Signer security roles FIA_UID.2/Signature User identification before any action	Section 7.2.1.3
O.Export_Signature_Électronique	FDP_IFC.1/Electronic signature export FDP_IFF.1/Electronic signature export FDP_ETC.2/Electronic signature export FMT_MSA.3/Electronic signature export FMT_SMF.1/Getting SCDev's signature generation status FMT_MSA.1/SCDev signature generation status FMT_SMR.1/Signer security roles FIA_UID.2/Signature User identification before any action	Section 7.2.1.3
O.Contrôle_Invariance_Sémantique_Du_Document	FDP_IFC.1/Document acceptance for signature FDP_IFC.1/Document acceptance for verifying FDP_IFF.1/Document acceptance for signature FDP_IFF.1/Document acceptance for verifying FDP_ITC.1/Document acceptance for signature FDP_ITC.1/Document acceptance for verifying FMT_MSA.3/Document's acceptance for signature FMT_MSA.3/Document's acceptance for verifying FMT_MSA.1/Document's semantics invariance status for signature FMT_MSA.1/Document's semantics invariance status for	

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

	verifying FMT_SMF.1/Getting document's semantics invariance status for signature FMT_SMF.1/Getting document's semantics invariance status for verifying FMT_MSA.1/Signer agreement to sign an instable document FMT_SMF.1/Getting signer agreement to sign an instable document FMT_SMR.1/Signer security roles FMT_SMR.1/Verifier security roles FIA_UID.2/Signature User identification before any action FIA_UID.2/Verification User identification before any action	
O.Référence_De_Temps	FDP_IFC.1/Time reference FDP_IFF.1/Time reference FMT_MTD.1/Selection of the applied signature policy FMT_SMF.1/Selection of the applied signature policy FDP_ITC.2/Time reference FPT_TDC.1/Time reference FMT_MSA.3/Time reference FMT_MSA.1/Time reference FMT_MSA.1/Certificates FMT_MSA.1/Certificates' validation FMT_SMR.1/Verifier security roles FIA_UID.2/Verifiaction User identification before any action	Section 7.2.1.4
O.Chemin_De_Certification	FDP_IFC.1/Certification path FDP_ITC.2/Certification path FPT_TDC.1/Certificates FPT_TDC.1/Certificate revocation data FDP_IFF.1/Certification path FMT_MTD.1/Selection of the applied signature policy FMT_SMF.1/Selection of the applied signature policy FMT_MSA.3/Certification path FMT_MSA.1/Certificates	Section 7.2.1.4

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

	FMT_MSA.1/Certificates' validation data FMT_SMR.1/Verifier security roles FIA_UID.2/Verification User identification before any action	
O.Conformité_Des_Certificats	FDP_IFC.1/Certification path FDP_ITC.2/Certification path FPT_TDC.1/Certificates FPT_TDC.1/Certificate revocation data FDP_IFF.1/Certification path FMT_MTD.1/Selection of the applied signature policy FMT_SMF.1/Selection of the applied signature policy FMT_MSA.3/Certification path FMT_MSA.1/Certificates FMT_MSA.1/Certificates' validation data FMT_SMR.1/Verifier security roles FIA_UID.2/Verification User identification before any action	Section 7.2.1.4
O.Validité_Des_Certificats	FDP_IFC.1/Certification path FDP_ITC.2/Certification path FPT_TDC.1/Certificates FPT_TDC.1/Certificate revocation data FDP_IFF.1/Certification path FMT_MTD.1/Selection of the applied signature policy FMT_SMF.1/Selection of the applied signature policy FMT_MSA.3/Certification path FMT_MSA.1/Certificates FMT_MSA.1/Certificates' validation data FMT_SMR.1/Verifier security roles FIA_UID.2/Verification User identification before any action	Section 7.2.1.4
O.Conformité_Données_Validation	FDP_IFC.1/Certification path FDP_ITC.2/Certification path FPT_TDC.1/Certificates FPT_TDC.1/Certificate revocation data FDP_IFF.1/Certification path	Section 7.2.1.4

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

	FMT_MTD.1/Selection of the applied signature policy FMT_SMF.1/Selection of the applied signature policy FMT_MSA.3/Certification path FMT_MSA.1/Certificates FMT_MSA.1/Certificates' validation data FMT_SMR.1/Verifier security roles FIA_UID.2/Verification User identification before any action	
O.Conformité_Attributs_Signés	FDP_IFC.1/Electronic signature validation FDP_IFF.1/Electronic signature validation FMT_MTD.1/Selection of the applied signature policy FMT_SMF.1/Selection of the applied signature policy FDP_ITC.2/Electronic signature FPT_TDC.1/Electronic signature FMT_MSA.3/Electronic signature FMT_MSA.1/Electronic signature FMT_SMR.1/Verifier security roles FIA_UID.2/Verification User identification before any action	Section 7.2.1.4
O.Communication_Attributs_Signés	FDP_IFF.1/Electronic signature	Section 7.2.1.4
O.Export_Données_Validation	FDP_IFC.1/Electronic signature validation FDP_IFF.1/Electronic signature validation FDP_ETC.2/Verification status FMT_MSA.3/Signature validation status FMT_MSA.1/Signature validation status FMT_SMR.1/Verifier security roles FIA_UID.2/Verification User identification before any action	Section 7.2.1.4
O.Invocation_Module_Contrôle_Invariance	FDP_IFC.1/Document acceptance for signature FDP_IFC.1/Document acceptance for verifying FDP_IFF.1/Document acceptance	

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

	for signature FDP_IFF.1/Document acceptance for verifying FDP_ITC.1/Document acceptance for signature FDP_ITC.1/Document acceptance for verifying FMT_MSA.3/Document's acceptance for signature FMT_MSA.3/Document's acceptance for verifying FMT_MSA.1/Document's semantics invariance status for signature FMT_MSA.1/Document's semantics invariance status for verifying FMT_SMF.1/Getting document's semantics invariance status for signature FMT_SMF.1/Getting document's semantics invariance status for verifying FMT_SMR.1/Signer security roles FMT_SMR.1/Verifier security roles FIA_UID.2/Signature User identification before any action FIA_UID.2/Verification User identification before any action	
O.Support_Cryptographique	FCS_COP.1/Hash Cryptographic operation FCS_COP.1/Signature verification	Section 7.2.1.4

Tableau 5 : Association des objectifs de sécurité de la TOE vers les exigences fonctionnelles

Exigences fonctionnelles pour la TOE	Objectifs de sécurité
FDP_IFC.1/Document acceptance for signature	O.Contrôle_Invariance_Sémantique_Du_Document O.Invocation_Module_Contrôle_Invariance
FDP_IFC.1/Document acceptance for verifying	O.Contrôle_Invariance_Sémantique_Du_Document O.Invocation_Module_Contrôle_Invariance
FDP_IFF.1/Document acceptance for signature	O.Contrôle_Invariance_Sémantique_Du_Document O.Invocation_Module_Contrôle_Invariance

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

FDP_IFF.1/Document acceptance for verifying	O.Contrôle_Invariance_Sémantique_Du_Document O.Invocation_Module_Contrôle_Invariance
FDP_ITC.1/Document acceptance for signature	O.Contrôle_Invariance_Sémantique_Du_Document O.Invocation_Module_Contrôle_Invariance
FDP_ITC.1/Document acceptance for verifyng	O.Contrôle_Invariance_Sémantique_Du_Document O.Invocation_Module_Contrôle_Invariance
FMT_MSA.3/Document's acceptance for signature	O.Contrôle_Invariance_Sémantique_Du_Document O.Invocation_Module_Contrôle_Invariance
FMT_MSA.3/Document's acceptance for verifying	O.Contrôle_Invariance_Sémantique_Du_Document O.Invocation_Module_Contrôle_Invariance
FMT_MSA.1/Selected documents	O.Ensemble_De_Documents_A_Signer
FMT_SMF.1/Selection of a list of documents	O.Ensemble_De_Documents_A_Signer
FMT_MSA.1/Document's semantics invariance status for signature	O.Contrôle_Invariance_Sémantique_Du_Document O.Invocation_Module_Contrôle_Invariance
FMT_MSA.1/Document's semantics invariance status for verifying	O.Contrôle_Invariance_Sémantique_Du_Document O.Invocation_Module_Contrôle_Invariance
FMT_SMF.1/Getting document's semantics invariance status for signature	O.Contrôle_Invariance_Sémantique_Du_Document O.Invocation_Module_Contrôle_Invariance
FMT_SMF.1/Getting document's semantics invariance status for verifying	O.Contrôle_Invariance_Sémantique_Du_Document O.Invocation_Module_Contrôle_Invariance
FMT_MSA.1/Signer agreement to sign an instable document	O.Contrôle_Invariance_Sémantique_Du_Document
FMT_SMF.1/Getting signer agreement to sign an instable document	O.Contrôle_Invariance_Sémantique_Du_Document
FDP_ROL.2/Abort of the signature process	O.Abandon_Du_Processus_De_Signature
FMT_MSA.1/Signature attributes	O.Ensemble_De_Documents_A_Signer O.Conformité_Des_Attributs
FMT_SMF.1/Modification of signature attributes	O.Ensemble_De_Documents_A_Signer O.Conformité_Des_Attributs
FDP_IFC.1/Signer's certificate import	O.Conformité_Du_Certificat O.Validité_Du_Certificat
FDP_IFF.1/Signer's certificate import	O.Conformité_Du_Certificat O.Validité_Du_Certificat
FMT_MSA.3/Signer's certificate import	O.Conformité_Du_Certificat

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

	O.Validité_Du_Certificat
FMT_MSA.1/Signer's certificate	O.Conformité_Du_Certificat O.Validité_Du_Certificat
FDP_ITC.2/Signer's certificate	O.Conformité_Du_Certificat O.Validité_Du_Certificat
FPT_TDC.1/Signer's certificate	O.Validité_Du_Certificat
FMT_SMF.1/Signer's certificate selection	O.Conformité_Du_Certificat O.Validité_Du_Certificat
FDP_IFC.1/Signature generation	O.Conformité_Des_Attributs
FDP_IFF.1/Signature generation	O.Association_Certificat/Clé_privée O.Conformité_Des_Attributs
FMT_MSA.3/Signature generation	O.Conformité_Des_Attributs
FDP_ITC.1/Explicit signer agreement	O.Consentement_Explicite
FDP_IFC.1/Electronic signature export	O.Export_Signature_Électronique
FDP_IFF.1/Electronic signature export	O.Export_Signature_Électronique
FDP_ETC.2/Electronic signature export	O.Export_Signature_Électronique
FMT_MSA.3/Electronic signature	O.Export_Signature_Électronique O.Conformité_Des_Attributs_Signés
FMT_MSA.1/SCDev signature generation status	O.Export_Signature_Électronique
FMT_SMF.1/Getting SCDev's signature generation status	O.Export_Signature_Électronique
FMT_SMR.1/Signer security roles et	O.Administration O.Conformité_Du_Certificat O.Validité_Du_Certificat O.Conformité_Des_Attributs O.Export_Signature_Électronique
FMT_SMR.1/Verifier security roles	O.Administration O.Référence_De_Temps O.Chemin_De_Certification O.Conformité_Des_Certificats O.Validité_Des_Certificats O.Conformité_Données_Validation O.Conformité_Des_Attributs_Signés O.Export_Données_Validation
FIA_UID.2/Signature User identification before any action	O.Conformité_Du_Certificat O.Validité_Du_Certificat O.Conformité_Des_Attributs

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

	O.Export_Signature_Électronique
FIA_UID.2/Verification User identification before any action	O.Référence_De_Temps O.Chemin_De_Certification O.Conformité_Des_Certificats O.Validité_Des_Certificats O.Conformité_Données_Validation O.Conformité_Des_Attributs_Signés O.Export_Données_Validation
FMT_MTD.1/Document format/viewer association table Management	O.Administration O.Lancement_d'Applications_De_Présentation
FMT_SMF.1/Management of the document format/viewer association table for signature	O.Administration O.Lancement_d'Applications_De_Présentation
FMT_SMF.1/Management of the document format/viewer association table for verifying	O.Administration O.Lancement_d'Applications_De_Présentation
FMT_MTD.1/Management of the signature policies	O.Administration
FMT_SMF.1/Management of the signature policies	O.Administration
FDP_IFC.1/Document acceptance for signature	O.Contrôle_Invariance_Sémantique_Du_Document O.Invocation_Module_Contrôle_Invariance
FDP_IFC.1/Document acceptance for verifying	O.Contrôle_Invariance_Sémantique_Du_Document O.Invocation_Module_Contrôle_Invariance
FDP_IFF.1/Document acceptance for signature	O.Contrôle_Invariance_Sémantique_Du_Document O.Invocation_Module_Contrôle_Invariance
FDP_IFF.1/Document acceptance for verifying	O.Contrôle_Invariance_Sémantique_Du_Document O.Invocation_Module_Contrôle_Invariance
FDP_ITC.1/Document acceptance for signature	O.Contrôle_Invariance_Sémantique_Du_Document O.Invocation_Module_Contrôle_Invariance
FDP_ITC.1/Document acceptance for verifying	O.Contrôle_Invariance_Sémantique_Du_Document O.Invocation_Module_Contrôle_Invariance
FMT_MSA.3/Document's acceptance for signature	O.Contrôle_Invariance_Sémantique_Du_Document O.Invocation_Module_Contrôle_Invariance
FMT_MSA.3/Document's acceptance for	O.Contrôle_Invariance_Sémantique_Du_Doc

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

verifying	ument O.Invocation_Module_Contrôle_Invariance
FMT_MSA.1/Document's semantics invariance status for signature	O.Contrôle_Invariance_Sémantique_Du_Document O.Invocation_Module_Contrôle_Invariance
FMT_MSA.1/Document's semantics invariance status for verifying	O.Contrôle_Invariance_Sémantique_Du_Document O.Invocation_Module_Contrôle_Invariance
FMT_SMF.1/Getting document's semantics invariance status for signature	O.Contrôle_Invariance_Sémantique_Du_Document O.Invocation_Module_Contrôle_Invariance
FMT_SMF.1/Getting document's semantics invariance status for verifying	O.Contrôle_Invariance_Sémantique_Du_Document O.Invocation_Module_Contrôle_Invariance
FMT_MTD.1/Document format/viewer association table management	O.Administration O.Lancement_d'Applications_De_Présentation
FMT_SMF.1/Management of the document format/viewer association table for signature	O.Administration O.Lancement_d'Applications_De_Présentation
FMT_SMF.1/Management of the document format/viewer association table for verifying	O.Administration O.Lancement_d'Applications_De_Présentation
FMT_MTD.1/Viewer activation parameter	O.Lancement_d'Applications_De_Présentation
FMT_SMF.1/Management of the viewer activation parameter	O.Lancement_d'Applications_De_Présentation
FMT_MTD.1/Selection of the applied signature policy	O.Référence_De_Temps O.Chemin_De_Certification O.Conformité_Des_Certificats O.Validité_Des_Certificats O.Conformité_Données_Validation O.Conformité_Des_Attributs_Signés
FMT_SMF.1/Selection of the applied signature policy	O.Référence_De_Temps O.Chemin_De_Certification O.Conformité_Des_Certificats O.Validité_Des_Certificats O.Conformité_Données_Validation O.Conformité_Des_Attributs_Signés
FDP_IFC.1/Electronic signature validation	O.Export_Signature_Électronique O.Conformité_Des_Attributs_Signés O.Export_Données_Validation
FDP_IFF.1/Electronic signature validation	O.Export_Signature_Électronique O.Communication_Attributs_Signés

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

	O.Conformité_Des_Attributs_Signés O.Export_Données_Validation
FDP_ETC.2/Verification status	O.Export_Données_Validation
FMT_MSA.3/Signature validation status	O.Export_Données_Validation
FMT_MSA.1/Signature validation status	O.Export_Données_Validation
FMT_MSA.1/Electronic signature	O.Conformité_Des_Attributs_Signés
FDP_ITC.2/Electronic signature	O.Conformité_Des_Attributs_Signés
FDP_IFC.1/Time reference	O.Référence_De_Temps
FDP_IFF.1/Time reference	O.Référence_De_Temps
FMT_MSA.3/Time reference	O.Référence_De_Temps
FMT_MSA.1/Time reference	O.Référence_De_Temps
FDP_ITC.2/Time reference	O.Référence_De_Temps
FMT_MSA.1/Certificates	O.Référence_De_Temps O.Chemin_De_Certification O.Conformité_Des_Certificats O.Validité_Des_Certificats O.Conformité_Données_Validation
FMT_MSA.1/Certificates' validation data	O.Référence_De_Temps O.Chemin_De_Certification O.Conformité_Des_Certificats O.Validité_Des_Certificats O.Conformité_Données_Validation
FDP_IFC.1/Certification path	O.Chemin_De_Certification O.Conformité_Des_Certificats O.Validité_Des_Certificats O.Conformité_Données_Validation
FDP_IFF.1/Certification path	O.Chemin_De_Certification O.Conformité_Des_Certificats O.Validité_Des_Certificats O.Conformité_Données_Validation
FMT_MSA.3/Certification path	O.Chemin_De_Certification O.Conformité_Des_Certificats O.Validité_Des_Certificats O.Conformité_Données_Validation
FDP_ITC.2/Certification path	O.Chemin_De_Certification O.Conformité_Des_Certificats O.Validité_Des_Certificats O.Conformité_Données_Validation

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

FPT_TDC.1/Electronic signature	O.Conformité_Des_Attributs_Signés
FPT_TDC.1/Time reference	O.Référence_De_Temps
FPT_TDC.1/Certificates	O.Chemin_De_Certification O.Conformité_Des_Certificats O.Validité_Des_Certificats O.Conformité_Données_Validation
FPT_TDC.1/Certificate revocation data	O.Chemin_De_Certification O.Conformité_Des_Certificats O.Validité_Des_Certificats O.Conformité_Données_Validation
FDP_IFC.1/Electronic signature validation	O.Conformité_Des_Attributs_Signés
FDP_IFF.1/Electronic signature validation	O.Conformité_Des_Attributs_Signés
FCS_COP.1/Signature verification	O.Support_Cryptographique
FCS_COP.1/Hash Cryptographic operation	O.Support_Cryptographique

Tableau 6 : Association exigences fonctionnelles vers objectifs de sécurité de la TOE

7.3 Dépendances

7.3.1 Dépendances des exigences de sécurité fonctionnelles

Exigences	Dépendances	Dépendances satisfaites
FDP_IFC.1/Document acceptance for signature	(FDP_IFF.1)	FDP_IFF.1/Document acceptance for signature
FDP_IFC.1/Document acceptance for verifying	(FDP_IFF.1)	FDP_IFF.1/Document acceptance for verifying
FDP_IFF.1/Document acceptance for signature	(FDP_IFC.1) et (FMT_MSA.3)	FDP_IFC.1/Document acceptance for signature, FMT_MSA.3/Document's acceptance for signature
FDP_IFF.1/Document acceptance for verifying	(FDP_IFC.1) et (FMT_MSA.3)	FDP_IFC.1/Document acceptance for verifying, FMT_MSA.3/Document's acceptance for verifying
FDP_ITC.1/Document acceptance for signature	(FDP_ACC.1 ou FDP_IFC.1) et	FDP_IFC.1/Document acceptance for signature,

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

	(FMT_MSA.3)	FMT_MSA.3/Document's acceptance for signature
FDP_ITC.1/Document acceptance for verifying	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_MSA.3)	FDP_IFC.1/Document acceptance for verifying, FMT_MSA.3/Document's acceptance for verifying
FMT_MSA.3/Document's acceptance for signature	(FMT_MSA.1) et (FMT_SMR.1)	FMT_MSA.1/Document's semantics invariance status for signature, FMT_SMR.1/Signer security roles
FMT_MSA.3/Document's acceptance for verifying	(FMT_MSA.1) et (FMT_SMR.1)	FMT_MSA.1/Document's semantics invariance status for verifying, FMT_SMR.1/Verifier security roles
FMT_MSA.1/Selected documents	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FMT_SMR.1/Signer security roles, FDP_IFC.1/Document acceptance, FMT_SMF.1/Selection of a list of documents
FMT_SMF.1/Selection of a list of documents	Pas de dépendance	
FMT_MSA.1/Document's semantics invariance status for signature	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FDP_IFC.1/Document acceptance for signature, FMT_SMF.1/Getting document's semantics invariance status for signature, FMT_SMR.1/Signer security roles
FMT_MSA.1/Document's semantics invariance status for verifying	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FDP_IFC.1/Document acceptance for verifying, FMT_SMF.1/Getting document's semantics invariance status for verifying, FMT_SMR.1/Verifier security roles
FMT_SMF.1/Getting document's semantics invariance status for signature	Pas de dépendance	
FMT_SMF.1/Getting document's semantics invariance status for verifying	Pas de dépendance	
FMT_MSA.1/Signer agreement	(FDP_ACC.1 ou	FMT_SMR.1/Signer security

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

to sign an instable document	FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	roles, FDP_IFC.1/Document acceptance, FMT_SMF.1/Getting signer agreement to sign an instable document
FMT_SMF.1/Getting signer agreement to sign an instable document	Pas de dépendance	
FDP_ROL.2/Abort of the signature process	(FDP_ACC.1 ou FDP_IFC.1)	FDP_IFC.1/Signature generation
FMT_MSA.1/Signature attributes	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FDP_IFC.1/Signature generation, FMT_SMR.1/Signer security roles, FMT_SMF.1/Modification of signature attributes
FMT_SMF.1/Modification of signature attributes	Pas de dépendance	
FDP_IFC.1/Signer's certificate import	(FDP_IFF.1)	FDP_IFF.1/Signer's certificate import
FDP_IFF.1/Signer's certificate import	(FDP_IFC.1) et (FMT_MSA.3)	FDP_IFC.1/Signer's certificate import, FMT_MSA.3/Signer's certificate import
FMT_MSA.3/Signer's certificate import	(FMT_MSA.1) et (FMT_SMR.1)	FMT_SMR.1/Signer security roles, FMT_MSA.1/Signer's certificate
FMT_MSA.1/Signer's certificate	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FMT_SMR.1/Signer security roles, FDP_IFC.1/Signer's certificate import, FMT_SMF.1/Signer's certificate selection
FDP_ITC.2/Signer's certificate	(FDP_ACC.1 ou FDP_IFC.1) et (FPT_TDC.1) et (FTP_ITC.1 ou FTP_TRP.1)	FDP_IFC.1/Signer's certificate import, FPT_TDC.1/Signer's certificate
FPT_TDC.1/Signer's certificate	Pas de dépendance	
FMT_SMF.1/Signer's certificate selection	Pas de dépendance	
FDP_IFC.1/Signature generation	(FDP_IFF.1)	FDP_IFF.1/Signature generation
FDP_IFF.1/Signature generation	(FDP_IFC.1) et (FMT_MSA.3)	FDP_IFC.1/Signature generation, FMT_MSA.3/Signature

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

		generation
FMT_MSA.3/Signature generation	(FMT_MSA.1) et (FMT_SMR.1)	FMT_SMR.1/Signer security roles, FMT_MSA.1/Signature attributes, FMT_MSA.1/Signer's certificate
FDP_ITC.1/Explicit signer agreement	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_MSA.3)	FDP_IFC.1/Signature generation, FMT_MSA.3/Signature generation
FDP_IFC.1/Electronic signature export	(FDP_IFF.1)	FDP_IFF.1/Electronic signature export
FDP_IFF.1/Electronic signature export	(FDP_IFC.1) et (FMT_MSA.3)	FDP_IFC.1/Electronic signature export, FMT_MSA.3/Electronic signature export
FDP_ETC.2/Electronic signature export	(FDP_ACC.1 ou FDP_IFC.1)	FDP_IFC.1/Electronic signature export
FMT_MSA.3/Electronic signature export	(FMT_MSA.1) et (FMT_SMR.1)	FMT_MSA.1/SCDev signature generation status, FMT_SMR.1
FMT_MSA.1/SCDev signature generation status	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FDP_IFC.1/Electronic signature export, FMT_SMF.1/Getting SCDev's signature generation status, FMT_SMR.1/Signer security roles
FMT_SMF.1/Getting SCDev's signature generation status	Pas de dépendance	
FCS_COP.1/Hash function Cryptographic operation	(FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2) et (FCS_CKM.4)	
FMT_SMR.1/Signer security roles	(FIA_UID.1)	FIA_UID.2/Signature User identification before any action
FMT_SMR.1/Verifier security roles	(FIA_UID.1)	FIA_UID.2/ Verification User identification before any action
FIA_UID.2/Signature User identification before any action	Pas de dépendance	
FIA_UID.2/Verification User identification before any action	Pas de dépendance	
FMT_MTD.1/Document format/viewer association table Management	(FMT_SMF.1) et (FMT_SMR.1)	FMT_SMF.1/Management of the document format/viewer association table, FMT_SMR.1/Signer

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

		security roles, FMT_SMR.1/Verifier security roles
FMT_SMF.1/Management of the document format/viewer association table for signature	Pas de dépendance	
FMT_SMF.1/Management of the document format/viewer association table for verifying	Pas de dépendance	
FMT_MTD.1/Management of the signature policies	(FMT_SMF.1) et (FMT_SMR.1)	FMT_SMR.1/Signer security roles, FMT_SMF.1/Management of the signature policies
FMT_SMF.1/Management of the signature policies	Pas de dépendance	
FDP_IFC.1/Document acceptance for signature	(FDP_IFF.1)	FDP_IFF.1/Document acceptance for signature
FDP_IFC.1/Document acceptance for verifying	(FDP_IFF.1)	FDP_IFF.1/Document acceptance for verifying
FDP_IFF.1/Document acceptance for signature	(FDP_IFC.1) et (FMT_MSA.3)	FDP_IFC.1/Document acceptance for signature, FMT_MSA.3/Document's acceptance for signature
FDP_IFF.1/Document acceptance for verifying	(FDP_IFC.1) et (FMT_MSA.3)	FDP_IFC.1/Document acceptance for verifying, FMT_MSA.3/Document's acceptance for verifying
FDP_ITC.1/Document acceptance for signature	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_MSA.3)	FDP_IFC.1/Document acceptance for signature, FMT_MSA.3/Document's acceptance for signature
FDP_ITC.1/Document acceptance for verifying	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_MSA.3)	FDP_IFC.1/Document acceptance for verifying, FMT_MSA.3/Document's acceptance for verifying
FMT_MSA.3/Document's acceptance for signature	(FMT_MSA.1) et (FMT_SMR.1)	FMT_SMR.1/Signer security roles, FMT_MSA.1/Selected documents, FMT_MSA.1/Document's semantics invariance status for signature
FMT_MSA.3/Document's acceptance for verifying	(FMT_MSA.1) et (FMT_SMR.1)	FMT_SMR.1/Verifier security roles, FMT_MSA.1/Selected documents,

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

		FMT_MSA.1/Document's semantics invariance status for verifying
FMT_MSA.1/Document's semantics invariance status for signature	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FMT_SMR.1/Signer security roles, FDP_IFC.1/Document Acceptance for signature, FMT_SMF.1/Getting document's semantics invariance status for signature
FMT_MSA.1/Document's semantics invariance status for verifying	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FMT_SMR.1/Verifier security roles, FDP_IFC.1/Document Acceptance for verifying, FMT_SMF.1/Getting document's semantics invariance status for verifying
FMT_SMF.1/Getting document's semantics invariance status for signature	Pas de dépendance	
FMT_SMF.1/Getting document's semantics invariance status for verifying	Pas de dépendance	
FMT_SMF.1/Management of the document format/viewer association table for signature	Pas de dépendance	
FMT_SMF.1/Management of the document format/viewer association table for verifying	Pas de dépendance	
FMT_MTD.1/Viewer activation parameter	(FMT_SMF.1) et (FMT_SMR.1)	FMT_SMF.1/Management of the viewer activation parameter, FMT_SMR.1/Signer security roles
FMT_SMF.1/Management of the viewer activation parameter	Pas de dépendance	
FMT_MTD.1/Selection of the applied signature policy	(FMT_SMF.1) et (FMT_SMR.1)	FMT_SMR.1/Verifier Security roles, FMT_SMF.1/Selection of the applied signature policy
FMT_SMF.1/Selection of the applied signature policy	Pas de dépendance	
FDP_IFC.1/Electronic signature	(FDP_IFF.1)	FDP_IFF.1/Electronic signature
FDP_IFF.1/Electronic signature	(FDP_IFC.1) et (FMT_MSA.3)	FDP_IFC.1/Electronic signature, FMT_MSA.3/Electronic signature

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

FMT_MSA.3/Electronic signature	(FMT_MSA.1) et (FMT_SMR.1)	FMT_SMR.1/Signer security roles, FMT_MSA.1/Electronic signature
FMT_MSA.1/Electronic signature	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FMT_SMR.1/Signer security roles, FDP_IFC.1/Electronic signature
FDP_ITC.2/Electronic signature	(FDP_ACC.1 ou FDP_IFC.1) et (FPT_TDC.1) et (FTP_ITC.1 ou FTP_TRP.1)	FDP_IFC.1/Electronic signature, FPT_TDC.1/Electronic signature
FDP_IFC.1/Time reference	(FDP_IFF.1)	FDP_IFF.1/Time reference
FDP_IFF.1/Time reference	(FDP_IFC.1) et (FMT_MSA.3)	FDP_IFC.1/Time reference, FMT_MSA.3/Time reference
FMT_MSA.3/Time reference	(FMT_MSA.1) et (FMT_SMR.1)	FMT_SMR.1/Verifier security roles, FMT_MSA.1/Time reference, FMT_MSA.1/Certificates, FMT_MSA.1/Certificates' validation data
FMT_MSA.1/Time reference	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FMT_SMR.1/Verifier security roles, FDP_IFC.1/Time reference
FDP_ITC.2/Time reference	(FDP_ACC.1 ou FDP_IFC.1) et (FPT_TDC.1) et (FTP_ITC.1 ou FTP_TRP.1)	FDP_IFC.1/Time reference, FPT_TDC.1/Time reference, FPT_TDC.1/Certificates, FPT_TDC.1/Certificate revocation data
FMT_MSA.1/Certificates	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FMT_SMR.1/Verifier security roles, FDP_IFC.1/Certification path
FMT_MSA.1/Certificates' validation data	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FMT_SMR.1/Verifier security roles, FDP_IFC.1/Certification path
FDP_IFC.1/Certification path	(FDP_IFF.1)	FDP_IFF.1/Certification path
FDP_IFF.1/Certification path	(FDP_IFC.1) et (FMT_MSA.3)	FDP_IFC.1/Certification path, FMT_MSA.3/Certification path
FMT_MSA.3/Certification path	(FMT_MSA.1) et	FMT_SMR.1/Verifier security

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

	(FMT_SMR.1)	roles, FMT_MSA.1/Certificates, FMT_MSA.1/Certificates' validation data
FDP_ITC.2/Certification path	(FDP_ACC.1 ou FDP_IFC.1) et (FPT_TDC.1) et (FTP_ITC.1 ou FTP_TRP.1)	FDP_IFC.1/Certification path, FPT_TDC.1/Certificates, FPT_TDC.1/Certificate revocation data
FPT_TDC.1/Electronic signature	Pas de dépendance	
FPT_TDC.1/Time reference	Pas de dépendance	
FPT_TDC.1/Certificates	Pas de dépendance	
FPT_TDC.1/Certificate revocation data	Pas de dépendance	
FDP_IFC.1/Electronic signature validation	(FDP_IFF.1)	FDP_IFF.1/Electronic signature validation
FDP_IFF.1/Electronic signature validation	(FDP_IFC.1) et (FMT_MSA.3)	FDP_IFC.1/Electronic signature validation, FMT_MSA.3/Signature validation status
FDP_ETC.2/Verification status	(FDP_ACC.1 ou FDP_IFC.1)	FDP_IFC.1/Electronic signature validation
FMT_MSA.3/Signature validation status	(FMT_MSA.1) et (FMT_SMR.1)	FMT_SMR.1/Verifier security roles, FMT_MSA.1/Signature validation status
FMT_MSA.1/Signature validation status	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FMT_SMR.1/Verifier security roles, FDP_IFC.1/Electronic signature validation
FCS_COP.1/Signature verification	(FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2) et (FCS_CKM.4)	FDP_ITC.2/Certification path
FCS_COP.1/Hash Cryptographic operation	(FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2) et (FCS_CKM.4)	

7.3.2 Argumentaire pour les dépendances non satisfaites

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

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

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

La dépendance FTP_ITC.1 or FTP_TRP.1 de FDP_ITC.2/Signer's certificate n'est pas supportée. La dépendance entre le composant d'exigence FDP_ITC.2/Signer's certificate et un des composants FTP_ITC.1 ou TFP_TRP.1 n'est pas satisfaite car les protocoles utilisés dans les infrastructures à clé publiques sont auto protégés et garantis, non pas immédiatement, mais au moment de la vérification de la signature:

- l'intégrité des certificats de la chaine de certification est garantie grâce au certificat auto signé (ou point de confiance) défini dans la politique de signature, qui est, elle-même maintenue intègre par l'environnement de la TOE
- lors de la vérification de la signature, le fait de construire une chaine de certification valide entre le certificat du signataire et le point de confiance défini dans la politique de signature permet à lui seul de garantir l'authenticité de l'origine des différents certificats composant cette chaine.
- enfin, le certificat du signataire, ne nécessite pas de protection en termes de confidentialité.

La dépendance FCS_CKM.4 de FCS_COP.1/Signature verification n'est pas supportée. La dépendance entre FCS_COP.1/Signature verification et FCS_CKM.4 n'est pas satisfaite, puisque les clés utilisées étant des clés publiques elles ne nécessitent pas de méthode sécurisée pour leur destruction.

La dépendance FCS_CKM.4 de FCS_COP.1/Hash Cryptographic operation **n'est pas supportée.** La dépendance entre le composant FCS_COP.1/Hash Cryptographic operation et le composant FCS_CKM.4 n'est pas satisfaite car un algorithme de hachage ne nécessite pas de clé, donc ne requiert pas d'exigences décrivant les méthodes de destruction des clés.

La dépendance FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 de FCS_COP.1/Hash Cryptographic operation **n'est pas supportée.** La dépendance entre le composant FCS_COP.1/Hash Cryptographic operation et un des trois composants FCS_CKM.1, FDP_ITC.1 et FDP_ITC.2 n'est pas satisfaite car un algorithme de hachage ne nécessite pas de clé, donc ne requiert pas d'exigences décrivant les méthodes de génération ou d'import de clés.

La dépendance FMT_SMF.1 de FMT_MSA.1/Electronic signature n'est pas supportée. Le composant FMT_MSA.1/Electronic signature ne définissant pas de nouvelle fonctionnalité de gestion, la dépendance entre ce composant et le composant FMT_SMF.1 n'a pas besoin d'être satisfaite.

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

La dépendance FTP_ITC.1 or FTP_TRP.1 de FDP_ITC.2/Electronic signature n'est pas supportée. La dépendance entre le composant d'exigence FDP_ITC.2/Electronic signature et un des composant FTP_ITC.1 ou TFP_TRP.1 n'est pas satisfaite car:

- ces données ne nécessitent pas de protection en confidentialité;
- la validité de la signature numérique contenue dans la signature électronique garantit l'intégrité des toutes les données signées;
- enfin, la validité de la signature électronique (si elle est attestée à la fin du processus de vérification) prouve l'authenticité de l'origine de l'information.

La dépendance FMT_SMF.1 de FMT_MSA.1/Time reference n'est pas supportée. La dépendance entre le composant FMT_MSA.1/Time reference et le composant FMT_SMF.1 n'est pas satisfaite car ce premier composant ne définit pas de nouvelle fonction de gestion des attributs de sécurité.

La dépendance FTP_ITC.1 or FTP_TRP.1 de FDP_ITC.2/Time reference n'est pas supportée. La dépendance entre le composant d'exigence FDP_ITC.2/Certificates' validation data et un des composants FTP_ITC.1 ou FTP_TRP.1 n'a pas à être satisfaite car les données véhiculées par les protocoles utilisés dans les infrastructures à clé publique sont auto protégées:

- l'intégrité de la référence de temps est garantie par la signature numérique qui lui est associée;
- l'authenticité de l'origine de la référence de temps est garantie par la construction d'un chemin de certification valide entre la clé de l'unité d'horodatage et un point de confiance dédié à l'horodatage défini dans la politique de signature.
- enfin, les données reçues par la TOE ne nécessitent pas de protection en termes de confidentialité.

La dépendance FTP_ITC.1 or FTP_TRP.1 de FDP_ITC.2/Certification path n'est pas supportée. La dépendance entre le composant d'exigence FDP_ITC.2/Certification path et un des composants FTP_ITC.1 ou FTP_TRP.1 n'a pas à être satisfaite car les protocoles utilisés dans les infrastructures à clé publiques sont autoprotégés:

- l'intégrité de chacun des certificats de la chaîne de certification et des informations de non révocation est garantie par une signature numérique apposée par une autorité supérieure, le certificat autosigné racine étant référencé dans la politique de signature (protégée en intégrité par la TOE).
- le fait de construire une chaîne de certification valide entre le certificat du signataire et un point de confiance défini dans la politique de signature permet à lui seul de garantir l'authenticité de l'origine des différents certificats composant cette chaîne.
- les données reçues par la TOE ne nécessitent pas de protection en termes de confidentialité.

La dépendance FMT_SMF.1 de FMT_MSA.1/Signature validation status n'est pas supportée. La dépendance entre le composant FMT_MSA.1/Signature validation status et le composant FMT_SMF.1 n'est pas satisfaite car ce premier composant ne définit pas de nouvelle fonction de gestion des attributs de sécurité.

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

La dépendance FMT_SMF.1 de FMT_MSA.1/Certificates n'est pas supportée. Le composant FMT_MSA.1/Certificates ne définissant pas de nouvelle fonctionnalité de gestion, la dépendance entre ce composant et le composant FMT_SMF.1 n'a pas besoin d'être satisfaite.

La dépendance FMT_SMF.1 de FMT_MSA.1/Certificates' validation data n'est pas supportée. Le composant FMT_MSA.1/Certificates' validation data ne définissant pas de nouvelle fonctionnalité de gestion, la dépendance entre ce composant et le composant FMT_SMF.1 n'a pas besoin d'être satisfaite.

7.4 Argumentaire pour l'EAL

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

7.5 Argumentaire pour les augmentations à l'AEL

7.5.1 AVA_VAN.3 Focused vulnerability analysis

Augmentation requise par le processus de qualification standard

7.5.2 ALC_FLR.3 Systematic flaw remediation

Augmentation requise par le processus de qualification standard.

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

8 Résumé des spécifications de la TOE

8.1 Fonctions de sécurité

8.1.1 Fonction de signature

F.Signature

Cette fonction permet de réaliser une signature suivant l'un des formats standards suivants :

- CAdES (ETSI TS 101 733) : formats CAdES-BES, CAdES-EPES, CAdES-T, CAdES-C, CadES-X-L, CAdES-A ;
- XAdES (ETSI TS 101 903) : formats XAdES-BES, XAdES-EPS, XAdES-T, XAdES-C, XAdES-X-L et XAdES-A ;
- PAdES (ETSI TS 102 778) : format CadES ou CMS.

Elle prend en entrée les paramètres depuis l'application utilisatrice :

- Un document à signer, sous la forme de données brutes ;

Elle prend en entrée depuis la fonction de configuration **F.Administration_Configuration :**

- Le type MIME des données à signer ;
- La politique de signature à appliquer ;
- L'algorithme de signature à utiliser ;
- Le format de signature à utiliser et des paramètres spécifiques au format de signature (XAdES) : algorithme de canonisation, algorithme de transformation, URI référençant les données signées,…
- Le type de signature (en correspondance avec le format de signature) :
  - Enveloppée (XAdES et PAdES) ;
  - Enveloppante (XAdES et CAdES) ;
  - Détaché (XAdES et CAdES).
- Des attributs :
  - Lieu présumé de la signature ;
  - Rôle du signataire ;
  - Type d'engagement.
- Les URL des serveurs d'horodatage, et optionnellement des serveurs de validation de certificats (hors périmètre d'évaluation de la TOE) à utiliser

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

Elle prend aussi en entrée depuis la fonction de sélection du certificat **F.Selection_Certificat** :

- Le certificat à utiliser pour la signature du document ;

De même, elle prend en entrée de **F.Contrôle_Invariance_Sémantique** :

- Le statut du contrôle de stabilité sémantique ;

Elle réalise les traitements suivants :

- Elle crée une enveloppe ou formate les données à signer conforment au format et au type de signature demandé ;
-
- Elle demande au signataire de sélectionner le certificat de signature parmi ceux présents sur le SCDev, puis de s'authentifier pour accéder aux informations du SCDev par appel à la fonction d'authentification **F.Authentification** ;
- Elle demande l'accord explicite au signataire de la réalisation de la signature
- Elle calcule le condensé de ces données suivant l'algorithme de hachage sélectionné ;
- Elle formate le condensé suivant le format de signature choisi ;

Jusqu'à cette étape, le signataire a la possibilité d'interrompre le processus de signature. Lorsque le SCDev à produit la signature électronique dans cette fonction, le processus de signature est considéré comme complet et ne peut donc plus être annulé.

- Elle demande au SCDev de générer la signature avec la clé privée associé au certificat du signataire en utilisant **F.Communication_SCDev** ;
- Elle récupère la signature générée par le SCDev et l'incorpore dans l'enveloppe **F.Communication_SCDev** ;

Note : le traitement des opérations de signature s'arrête dès qu'une erreur se produit.

Elle retourne :

- Les données signées suivant le format de signature utilisé ;

  La signature contient en autre :

  - La signature numérique renvoyée par le SCDev ;
  - La valeur haché des données à signées et l'OID de l'algorithme utilisé ;
  - Le certificat de signature
  - La référence de la politique de signature utilisée (uniquement dans le cas d'une signature EPES)

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

- Un jeton d'horodatage (dans le cas d'une signature augmentée T, XL ou LTV)
- La référence aux certificats d'autorités de confiance et aux CRLs (dans le cas d'une signature augmentée XL ou LTV)

o Ou un code d'erreur si le processus de génération de signature n'a pas s'exécuter correctement.

Cette fonction est réalisée par l'utilisation de MetaSIGN-API.

8.1.2 Fonction de sélection de certificat

F.Selection_Certificat

MetaSIGN supporte 3 types d'interface pour accéder à la clé privée du signataire :

o PKCS #12 ;

o PKCS #11 ;

o MSCAPI.

Cette fonction présente uniquement les certificats en accord avec les informations contenues dans la politique de signature utilisée (restrictions sur les types d'usages de clés et sur les certificats d'autorités de confiance).

La TOE présente uniquement les certificats contenus dans le SCDev.

Elle demande au signataire de sélectionner un certificat de signature s'il y en a plusieurs possible ;

Cette fonction est réalisée par l'utilisation de MetaSIGN-API.

8.1.3 Fonction de contrôle d'invariance sémantique

F.Contrôle_Invariance_Sémantique

Cette fonction invoque un module externe de contrôle d'invariance suivant le type MIME des données à signer (un module par type MIME), en lui passant en argument les données à signer.

Le module appelé retourne un statut du contrôle de stabilité sémantique.

Si la sémantique du document est instable, la fonction retourne une erreur en fonction de la politique de signature utilisée qui peut ou pas accepter l'instabilité d'un document pour sa signature ou sa vérification..

8.1.4 Fonction d'authentification

F.Authentification

Cette fonction permet de réaliser l'authentification de l'utilisateur avant toute action de signature.

Cette fonction appelle la fonction d'authentification du SCDev configuré par la fonction d'administration et de configuration **F.Administration_Configuration**, en lui passant

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

optionnellement en paramètre le code PIN ou mot de passe déverrouillant le SCDev (géré par l'interface PKCS #11, CMS, ou PKCS #12).

SI un PINpad est utilisé avec le SCDEv, le code PIN est saisi directement via le PINpad et ne transite pas à travers la TOE.

Cette fonction est réalisée par l'utilisation de MetaSIGN-API.

8.1.5 Fonction application de politique de signature

F_APPLICATION_Politique_Signature

La politique de signature est composée des données suivantes :

- Le nom et la description textuelle de la politique de signature ;
- L'identifiant unique (OID) de la politique de signature ;
- L'identifiant des fonctions de hachage utilisables ;
- Les certificats des AC Racines de confiances autorisées pour le certificat du signataire ;
- Les valeurs autorisées de l'extension « certificatePolicies » du certificat du signataire et de la racine ;
- Mode de tests de la révocation du certificat du signataire et de la validité des CRLs uniquement lors de la vérification de signature ;
- Les valeurs autorisées de l'extension « keyUsage » du certificat du signataire : présence des bits digital signature et non répudiation ;
- Période de grâce pour le certificat du signataire ;
- Les types d'engagements acceptés et le type choisi par défaut ;
- Les certificats des AC Racines de confiances autorisées pour le certificat de l'autorité d'horodatage ;
- Les valeurs autorisées de l'extension « certificatePolicies » du certificat de l'autorité d'horodatage ;
- Mode de tests de la révocation du certificat de l'autorité d'horodatage et de la validité des CRLs uniquement lors de la vérification de signature ;
- Période de grâce pour le certificat de l'autorité d'horodatage.

Les politiques de signatures sont localisées dans un magasin de politiques, défini par l'administrateur (assuré par l'application utilisatrice) de la TOE.

La fonction **F.Administration_Configuration** fournit la localisation du magasin des politiques de signatures.

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

Les fonctions **F.Signature** et **F.Verification_Signature** fournissent l'identifiant de la politique de signature à utiliser pour une opération de signature ou de vérification.

Cette fonction est appliquée lors de la création de signature et lors de la vérification.

Lors de la vérification (**F.Verification_Signature**), si la signature à vérifier n'est pas conforme aux éléments contenus dans la politique, alors la signature sera déclarée invalide.

De même lors de la création (**F.Signature**), cette fonction ne permet pas la génération d'une signature non conforme aux éléments de contraintes sur les certificats contenus dans la politique de signature (certificat du signataire reconnu par une AC Racine identifiée dans la politique, extension « certificatePolicies » du certificat du signataire, extension « keyUsage » du certificat du signataire, période de grâce pour le certificat du signataire).

Cette fonction est réalisée par l'utilisation de MetaSIGN-API.

8.1.6 Fonction de présentation de document

F_Presentation_ Document

La TOE appelle un module externe permettant au signataire ou au vérificateur de visualiser le document à signer ou signé.

Suivant le type MIME du document à signer ou vérifier, la TOE lance le module externe de visualisation adapté (NotePad, WordPad, ou Acrobat Reader….).

8.1.7 Fonction de présentation des attributs

F.Présentation_Attributs

La TOE appelle un module externe permettant au signataire, lors de la signature, de visualiser les attributs de signature. Les attributs de signature pris en charge par la TOE sont les suivants :

- Le certificat du signataire ou son identifiant unique ;
- L'identifiant unique de la politique de signature ;
- Le type d'engagement du signataire ;
- Le rôle du signataire ;
- La date et l'heure présumée de la signature ;
- Le lieu présumé de la signature ;
- Le type MIME du document.

Cette fonction est réalisée par l'utilisation de MetaSIGN-API.

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

8.1.8 Fonction de comminication avec le SCDev

F.Communication_SCDev

Cette fonction permet à la TOE d'interagir avec le SCDev, en utilisant des composants logiciels et/ou matériels intermédiaires (middleware) hors du périmètre de la TOE.

Cette fonction permet :

- De gérer une session avec le SCDev (établir et fermer) ;
- D'obtenir du SCDev les références des certificats utilisables par le signataire, ou les certificats eux-mêmes ;
- D'indiquer au SCDev la clé de signature à activer ;
- De transférer au SCDev la représentation des données à signer. Il s'agit de la valeur hachée des données à signer ;
- Demande au SCDev de générer la signature de la valeur hachée des données à signer en utilisant la clé privée du certificat de signature ;
- Pour chaque document à signer, de recevoir du SCDev la signature numérique ainsi que le statut d'exécution associé ;
- De vérifier que la signature reçue du SCDev est bien au format PKCS#1.

Cette fonction est réalisée par l'utilisation de MetaSIGN-API.

8.1.9 Fonction Administration et configuration

F.Administration_Configuration

Cette fonction permet à l'administrateur (assuré par l'application utilisatrice) de définir les paramètres de configuration de l'applet utilisée.

Le paramétrage est regroupé en sous-ensembles :

- Les paramètres de définition de l'IHM
- Les paramètres de configuration du module d'invariance sémantique ;
- Les paramètres de configuration du module de visualisation des documents ;
- Les paramètres de configuration de l'utilisation de MetaSIGN-API :
  - Les paramètres de contexte d'utilisation (la politique de signature, URLs du serveur d'horodatage, magasins pour les politiques de confiance, les politiques externes, les magasins des certificats d'Autorités de Certificats et des CRLS, l'URL du serveur d'archivage, le « provider » PKCS#11 utilisé pour communiquer avec le SCDev, la durée de vie maximale de conservation des fichiers temporaires).

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

- Les paramètres destinés à la génération de la signature (type de signature, algorithmes de signature, de canonisation et de transformation.)
- Les propriétés de la signature (engagement du signataire, type et format d'encodage des données, lieu de signature, rôle du signataire, attributs spécifiques liés à une signature PAdES).
- Les paramètres destinés à la vérification et l'augmentation de la signature (politique de signature utilisée pour la vérification, informations sur le type d'augmentation (T, C, XL ou LTV)).

8.1.10 Fonction de vérification de signature

F.Verification_Signature

Cette fonction permet de vérifier une signature réalisée dans un des formats standards suivants :

- CadES (ETSI TS 101 733) : formats CAdES-BES, CAdES-EPES, CAdES-T, CAdES-C, CAdES-X-L, et CAdES-A ;
- XAdES (ETSI TS 101 903) : formats XAdES-BES, XAdES-EPS, XAdES-T, XAdES-C et XAdES-X-L et XAdES-A ;
- PAdES (ETSI TS 102 778) : format CAdES, CMS ou LTV

Cette fonction est composée de deux opérations différentes (exclusive l'une de l'autre) :

- Vérification immédiate & optionnellement augmentation ;
- Vérification ultérieure.

Elle prend en entrée les paramètres depuis l'application utilisatrice suivants :

- La signature
- Les données signées (si non incluses dans la signature) ;

Elle prend en entrée depuis la fonction de configuration et de configuration
F.Administration_Configuration : La politique de signature à appliquer ;

- La politique de signature à appliquer ;
- L'opération de vérification à réaliser : vérification avec augmentation ou vérification ultérieure ;
- Le mode d'augmentation (par valeur ou par référence) dans le contexte de la vérification avec augmentation ;
- Les URL du serveur d'horodatage , et optionnellement du serveur de validation de certificats (hors périmètre d'évaluation de la TOE) ;
- Les magasins des certificats d'Autorités de Certificats et des CRLS

Elle réalise les traitements suivants :

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

- La vérification avec augmentation d'une signature électronique consiste à horodater puis à vérifier la validité d'une signature issue du module de génération, en vérifiant la validité et le statut de non révocation des certificats utilisés dans les chaines de certifications (à la date d'horodatage). Ensuite, une augmentation de la signature de toutes les valeurs nécessaires à la vérification ultérieure (certificats d'AC, CRLs) est réalisée si elle est demandée (format XL ou LTV). Cette vérification s'effectue par rapport à une politique de signature déterminée soit par la signature elle-même (cas d'une signature EPES) soit par la fonction **F.Administration_Configuration** (vérification de la conformité par rapport aux éléments constituant la politique de signature).
- La vérification ultérieure d'une signature électronique consiste à contrôler la signature par rapport à la politique de signature définie soit par la signature elle-même (cas d'une signature EPES) soit par la fonction **F.Administration_Configuration**. La vérification est réalisée en utilisant les éléments qui ont été stockés à l'intérieur de la signature suite à son augmentation. Elle peut être effectuée à tout moment, y compris après la date d'expiration du certificat du signataire. Cette vérification doit toutefois avoir lieu avant l'expiration du certificat de l'unit é d'horodatage du dernier jeton apposé sur la signature.

Note : Le processus de vérification de la signature s'arrête dès qu'un élément de la signature est non valide et engendre un statut global à « invalide »

Elle retourne :

- Un rapport de vérification comprenant :
  - Un statut global (valide/invalide/indéterminé) ;
  - Un statut détaillé présentant chaque élément vérifié (au format texte ou au format xml) ;
- Une nouvelle signature dans le cas d'une vérification avec augmentation.

Cette fonction est réalisée par l'utilisation de MetaSIGN-API.

8.2 Couverture des exigences fonctionnelles

F.Signature

Cette fonction couvre les exigences fonctionnelles suivantes :

Exigences fonctionnelles	Argumentaire de couverture
FDP_ROL.2/Abort of the	Le signataire peut interrompre l'opération de signature.

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

signature process	
FDP_ITC.1/Explicit signer agreement	Le signataire doit donner son accord pour signer un document
FDP_IFC.1/Electronic signature export	La TOE peut récupérer la signature générée par le SCDev et l'exporter
FDP_IFF.1/Electronic signature export	La TOE peut récupérer la signature générée par le SCDev et l'exporter
FDP_ETC.2/Electronic signature export	La TOE peut récupérer la signature générée par le SCDev et l'exporter
FMT_MSA.3/Electronic signature export	La signature exportée par la TOE n'est pas modifiable
FMT_SMR.1/Signer security roles	La fonction contribue à la couverture de l'exigence car elle fournit une interface séparée entre l'application utilisatrice de la TOE et le signataire
FCS_COP.1/Hash function Cryptographic operation	La fonction réalise le calcul de l'empreinte (haché) des données à signer par le SCDev

F.Selection_Certificat

Cette fonction couvre les exigences fonctionnelles suivantes :

Exigences fonctionnelles	**Argumentaire de couverture**
FDP_IFC.1/Signer's certificate import	Le signataire peut sélectionner son certificat à utiliser
FDP_IFF.1/Signer's certificate import	Le signataire peut sélectionner son certificat à utiliser
FMT_MSA.3/Signer's certificate import	Le signataire peut sélectionner son certificat à utiliser
FMT_MSA.1/Signer's certificate	Le signataire peut sélectionner son certificat à utiliser
FDP_ITC.2/Signer's certificate import	Le signataire peut sélectionner son certificat à utiliser
FPT_TDC.1/Signer's certificate	Le signataire peut sélectionner son certificat à utiliser
FMT_SMF.1/Signer's certificate selection	Le signataire peut sélectionner son certificat à utiliser
FMT_SMR.1/Signer security roles	La fonction contribue à la couverture de l'exigence car elle fournit une interface séparée entre l'application utilisatrice de la TOE et le signataire
FIA_UID.2/Signature User identification before any action	La fonction contribue à la couverture de l'exigence car elle fournit une interface séparée entre l'application utilisatrice de la TOE et le signataire

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

F.Contrôle_Invariance_Sémantique

Cette fonction couvre les exigences fonctionnelles suivantes :

Exigences fonctionnelles	Argumentaire de couverture
FDP_IFC.1/Document acceptance for signature	La stabilité du document est contrôlée avant sa signature
FDP_IFC.1/Document acceptance for verifying	La stabilité du document signé est contrôlée avant sa verification
FDP_IFF.1/Document acceptance for signature	La stabilité du document est contrôlée avant sa signature
FDP_IFF.1/Document acceptance for verifying	La stabilité du document signé est contrôlée avant sa vérification
FDP_ITC.1/Document acceptance for signature	Seuls les documents à signer dont la sémantique est invariable sont acceptés
FDP_ITC.1/Document acceptance for verifying	Seuls les documents à signer dont la sémantique est invariable sont acceptés
FMT_MSA.3/Document acceptance	Il est impossible de forcer la signature de documents non stables
FMT_MSA.1/Document's semantics invariance status	Il est impossible de forcer la signature de documents non stables
FMT_MSA.1/Selected Document	L'utilisateur peut sélectionner les documents à signer/à vérifier
FMT_SMF.1/Getting document's semantics invariance status	La TOE peut appeler une application externe pour vérifier la stabilité du document à signer
FMT_MSA.1/Signer agreement to sign an instable document	L'utilisateur doit donner son accord pour signer un document non stable
FMT_SMF.1/Getting signer agreement to sign an instable document	L'utilisateur doit donner son accord pour signer un document non stable

F.Authentification

Cette fonction couvre les exigences fonctionnelles suivantes :

Exigences fonctionnelles	Argumentaire de couverture

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

FIA_UID.2/Signature User identification before any action	Le signataire doit être identifié

F_Application_Politique_Signature

Cette fonction couvre les exigences fonctionnelles suivantes :

Exigences fonctionnelles	Argumentaire de couverture
FDP_IFF.1/Signer's certificate import	La fonction permet de filtrer la liste des certificats disponible en accord avec les paramètres de la politique de signature
FPT_TDC.1/Signer's certificate	La fonction permet de filtrer la liste des certificats disponible en accord avec les paramètres de la politique de signature
FDP_IFF.1/Signature generation	La fonction permet d'identifier les règles dans la politique de signature qui doivent être remplies pour permettre la génération de la signature. Les données à signer sont transférées au SCDev sous certaines conditions
FMT_MSA.3/Signature generation	La fonction permet d'identifier les règles dans la politique de signature qui doivent être remplies pour permettre la génération de la signature. Les données à signer sont transférées au SCDev sous certaines conditions

F_Presentation_ Document

Cette fonction couvre les exigences fonctionnelles suivantes :

Exigences fonctionnelles	Argumentaire de couverture
FDP_IFF.1/Signature generation	La fonction affiche le document à signer en accord avec son format
FMT_MTD.1/Document format/viewer association table Management	L'administrateur (assuré par l'application utilisatrice) peut modifier le choix de l'application à utiliser pour visionner les documents
FMT_SMF.1/Management of the document format/viewer association table for signature	L'administrateur (assuré par l'application utilisatrice) peut modifier le choix de l'application à utiliser pour visionner les documents à signer
FMT_SMF.1/Management of the document format/viewer association table for verifying	L'administrateur (assuré par l'application utilisatrice) peut modifier le choix de l'application à utiliser pour visionner les documents à verifier
FMT_MTD.1/viewer activation parameter	L'administrateur (assuré par l'application utilisatrice) peut modifier le paramètre d'activation du visualiseur
FMT_SMF.1/Management of the viewer	L'administrateur (assuré par l'application utilisatrice) peut modifier le paramètre d'activation du visualiseur

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

activation parameter	

F.Présentation_Attributs

Cette fonction couvre les exigences fonctionnelles suivantes :

Exigences fonctionnelles	Argumentaire de couverture
FDP_IFF.1/Signature generation	La fonction affiche à l'utilisateur les attributs de signature

F.Communication_SCDev

Cette fonction couvre les exigences fonctionnelles suivantes :

Exigences fonctionnelles	Argumentaire de couverture
FDP_IFC.1/Signer's certificate import	La fonction récupère depuis le SCDev la liste des certificats disponible
FDP_IFF.1/Signer's certificate import	La fonction récupère depuis le SCDev la liste des certificats disponible
FDP_IFC.1/Signature generation	La fonction requière que le SCDev réalise la signature numérique de l'empreinte (haché) avec la clé privée correspondant au certificat de signature
FDP_IFF.1/Signature generation	La fonction requière que le SCDev réalise la signature numérique de l'empreinte (haché) avec la clé privée correspondant au certificat de signature
FDP_IFF.1/Electronic signature export	La fonction contrôle que la signature générée par le SCDev est conforme à une signature PKCS#1
FMT_MSA.3/Electronic signature export	La fonction exporte la signature générée depuis le SCDev
FMT_MSA.1/SCDev signature generation status	La fonction exporte l'état de la génération de la signature qu'elle soit réussie ou en échec depuis le SCDev
FMT_SMF.1/Getting SCDev's signature generation status	La fonction exporte l'état de la génération de la signature qu'elle soit réussie ou en échec depuis le SCDev

F.Administration_Configuration

Cette fonction couvre les exigences fonctionnelles suivantes :

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

Exigences fonctionnelles	Argumentaire de couverture
FMT_MSA.1/Signature attributes	La fonction permet de définir (au travers de l'administration des politiques de signature), les attributs de signature
FMT_SMF.1/Modification of signature attributes	La fonction permet la configuration et la modification des attributs de signature (au travers de l'administration des politiques de signature)
FDP_ITC.1/Explicit signer agreement	La fonction permet de rendre obligatoire le consentement explicite du signataire
FMT_MTD.1/Management of the signature policies	La fonction permet de gérer le magasin des politiques de signature
FMT_SMF.1/Management of the signature policies	La fonction permet de gérer la politique de signature utilisée pour les opérations de signature et de vérification.
FMT_MTD.1/Selection of the applied signature policy	La fonction permet de gérer la politique de signature utilisée pour les opérations de signature et de vérification
FMT_SMF.1/Selection of the applied signature policy	La fonction permet de gérer la politique de signature utilisée pour les opérations de signature et de vérification
FDP_IFC.1/Time reference	La fonction permet de définir l'accès au service d'horodatage permettant d'obtenir une base de temps fiable
FDP_IFF.1/Time reference	La fonction permet de définir l'accès au service d'horodatage permettant d'obtenir une base de temps fiable
FMT_MSA.3/Time reference	La fonction permet de définir l'accès au service d'horodatage permettant d'obtenir une base de temps fiable L'horloge n'est pas altérable
FMT_MSA.1/Time reference	La fonction permet de définir l'accès au service d'horodatage permettant d'obtenir une base de temps fiable. L'horloge n'est pas altérable
FDP_ITC.2/Time reference	La fonction permet de définir l'accès au service d'horodatage permettant d'obtenir une base de temps fiable.
FMT_MSA.1/Certificates validation data	La fonction permet de définir l'accès aux magasins des certificats d'Autorités de Certificats et des
FDP_IFC.1/Certification path	La fonction permet de définir les chemins de certification d'un certificat (au travers de l'administration des politiques de signature)
FDP_IFF.1/Certification path	La fonction permet de définir les chemins de certification d'un certificat (au travers de l'administration des politiques de signature)
FMT_SMR.1/Signer Security roles	La fonction contribue à la couverture de l'exigence car elle permet à l'administrateur (assuré par l'application utilisatrice) de modifier les paramètres d'utilisation de la TOE
FMT_SMR.1/Verifier Security roles	La fonction contribue à la couverture de l'exigence car elle permet à l'administrateur (assuré par l'application utilisatrice) de modifier les paramètres d'utilisation de la TOE

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

F.Verification_Signature

Cette fonction couvre les exigences fonctionnelles suivantes :

Exigences fonctionnelles	Argumentaire de couverture
FMT_SMR.1/Verifier security roles	La fonction contribue à la couverture de l'exigence car elle fournit une interface séparée entre l'application utilisatrice de la TOE et le signataire
FIA_UID.2/Verification User identification before any action	La fonction contribue à la couverture de l'exigence car elle fournit une interface séparée entre l'application utilisatrice de la TOE et le signataire
FDP_IFC.1/Electronic signature validation	La fonction permet de récupérer le résultat de l'opération de vérification de signature
FDP_IFF.1/Electronic signature validation	La fonction permet de récupérer le résultat de l'opération de vérification de signature
FMT_MSA.3/Signature validation status	Personne ne peut altérer les résultats de l'opération de vérification de signature
FMT_MSA.1/Signature validation status	Personne ne peut altérer les résultats de l'opération de vérification de signature
FDP_ETC.2/Verification status	La fonction permet de récupérer le résultat de l'opération de vérification de signature
FDP_IFC.1/Time reference	La TOE permet d'importer une base de temps fiable
FDP_IFF.1/Time reference	La TOE permet d'importer une base de temps fiable
FMT_MSA.3/Time reference	L'horloge de référence n'est pas altérable
FMT_MSA.1/Time reference	L'horloge de référence n'est pas altérable
FDP_ITC.2/Time reference	La TOE permet d'importer une base de temps fiable
FMT_MSA.1/Certificates	Le chemin de certification n'est pas modifiable dans les certificats importés
FMT_MSA.1/Certificates' validation data	Le chemin de certification n'est pas modifiable dans les données de validation des certificats importés
FDP_IFC.1/Certification path	La TOE peut vérifier le chemin de certification d'un certificat
FDP_IFF.1/Certification path	La TOE peut vérifier le chemin de certification d'un certificat
FMT_MSA.3/Certification path	Les paramètres de vérification du chemin de certification ne sont pas altérables
FDP_ITC.2/Certification path	La TOE peut récupérer les données nécessaires à la vérification du chemin de certification

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

FPT_TDC.1/Electronic signature	Utilisation des standards ETSI CMS, CADES,XADES, PADES,
FPT_TDC.1/Time reference	Utilisation des standards RFC-3161
FPT_TDC.1/Certificates	Utilisation des standards X509 v3 standard
FPT_TDC.1/Certificate revocation data	Utilisation des standards CRL V2
FDP_IFC.1/Electronic signature validation	La TOE permet de récupérer les résultats de l'opération de vérification de signature
FDP_IFF.1/Electronic signature validation	La TOE permet de récupérer les résultats de l'opération de vérification de signature
FCS_COP.1/Signature verification	Opération de vérification de la signature
FCS_COP.1/Hash Cryptographic operation	La fonction réalise le calcul de l'empreinte (haché) des signées

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

9 Glossaire des Termes and Acronymes

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

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

9.1 Termes propres aux Critères Communs

Evaluation Assurance Level (EAL)

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

Target Of Evaluation (TOE)

En français, Cible d'évaluation.

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

TOE Security Policy (TSP)

En français, politique de sécurité de la TOE.

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

9.2 Termes propres à la signature électronique

Autorité de certification qualifiée

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

Certificat électronique

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

Un certificat électronique doit comporter :

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

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

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

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 ;

Certificat électronique qualifié

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

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

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

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

Condensé

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

Cryptographic Service Provider (CSP)

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

Dispositif de création de signature électronique

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

Dispositif sécurisé de création de signature électronique

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

Dispositif de vérification de signature électronique

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

Directive

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

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 presenter correctement le document.

Object Identifier (OID)

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

Politique de signature

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

Prestataire de services de certification électronique

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

Qualification des prestataires de services de certification électronique

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

particulières de qualité.

Signataire

Toute personne physique, agissant pour son propre compte ou pour celui de la personne

physique ou morale qu'elle représente, qui met en œuvre un dispositif de création de

signature électronique ;

Signature électronique

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

Signature électronique sécurisée

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

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

o être propre au signataire ;

o être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ;

o garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable ;

Signature électronique présumée fiable

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

On parle aussi de signature électronique qualifiée.

Signature numérique

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

Système de création de signature

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

9.3 Acronymes

ETSI	European Telecommunications Standards Institute
CWA	CEN Workshop Agreements
CSP	Cryptographic Service Provider.
TOE	Target of Evaluation, en français, cible d'évaluation
SCDev	Signature Creation Device
SFP	Security Function Policy
SSCD	Secure Signature Creation Device
PKCS#11	Public Key Cryptography Standards
OID	Object Identifier, en français identifiant d'objet.

9.4 Références

[CC1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 3.1, Revision 1, September 2006.

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS

[CC2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements. Version 3.1, Revision 2, September 2007.
[CC3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements. Version 3.1, Revision 2, September 2007.
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology. Version 3.1, Revision 2, September 2007.
[PP-ACSE-CCv3.1]	« Application de création de signature électronique » [PP-ACSE-CCv3.1], version 1.7 du 2 mars 2011
[PP-MVSE-CCv3.1]	« Module de vérification de signature électronique » [PP-MVSE-CCv3.1], version'1.7 du 2 mars 2011
[QUA-STD]	Processus de qualification d'**Erreur ! Référence de lien hypertexte non valide.**écurité – Niveau standard. Version 1.2 voir www.ssi.gouv.fr.
[CRYPT-STD]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques. ANSSI. voir www.ssi.gouv.fr
[AUTH-STD]	Authentification - Règles et recommandations concernant les mécanismes d'authentification. ANSSI. voir www.ssi.gouv.fr
[KEYS-STD]	Gestion de clés - Règles et recommandations concernant la gestion des clés utilisées dans les mécanismes cryptographiques. ANSSI. voir www.ssi.gouv.fr
[ETSI TS 101 733]	CMS Advanced Electronic Signature, définie dans la spécification technique (version 2.2.1) (2013-04)
[ETSI TS 101 903]	XAdES : XML Advanced Electronic Signature, définie dans la spécification technique (version 1.4.2) (2010-12)
[ETSI TS 102 778-3]	PDF Advanced Electronic Signature, définie dans la spécification technique ETSI TS 102 778-2 (version 1.2.1) (2009-07), TS 102 778-3 (version 1.2.1) (2010-07) et TS 102 778-4 (version 1.1.2) (2009-12)
[ETSI TR 102 038]	XML Format for signature policies, définie dans la spécification technique (version 1.1.1) (2002-04)

End of the document

Copyright 2015 Bull SAS

This document is the proprietary of Bull SAS and it can not be disclosed to a third party without a written approval
Ce document est la propriété de Bull et ne peut être divulgué à des parties tierces sans l'accord préalable de Bull SAS