Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

# Rapport de certification ANSSI-CC-2016/09

# MetaSIGN-API

# Version 3.3.5

*Paris, le 21 mars 2016*

*Le directeur général de l'agence nationale*
*de la sécurité des systèmes d'information*

Guillaume POUPARD
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

# Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification@ssi.gouv.fr

*Référence du rapport de certification*

# ANSSI-CC-2016/09

*Nom du produit*

# MetaSIGN-API

*Référence/version du produit*

# Version 3.3.5

*Critères d'évaluation et version*

# Critères Communs version 3.1 révision 3

*Niveau d'évaluation*

# EAL 3 augmenté

**ALC_FLR.3, AVA_VAN.3**

*Développeur*

# Bull SAS (Groupe Atos)

**rue Jean Jaurès, 78340 Les Clayes sous-bois, France**

*Commanditaire*

# Bull SAS (Groupe Atos)

**rue Jean Jaurès, 78340 Les Clayes sous-bois, France**

*Centre d'évaluation*

# Oppida

**4-6 avenue du vieil étang, Bâtiment B, 78180 Montigny le Bretonneux, France**

*Accords de reconnaissance applicables*

**CCRA**

**SOG-IS**

# Préface

## La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- L'agence nationale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont disponibles sur le site Internet www.ssi.gouv.fr.

# Table des matières

# 1. Le produit

## 1.1. Présentation du produit

Le produit évalué est « MetaSIGN-API v3.3.5 », bibliothèque en langage Java développée par *BULL SAS* (Groupe *ATOS*). Il fournit des services de génération et de vérification de signature électronique aux formats CadES (CMS *Advanced Electronic Signature*), XAdES (XML *Advanced Electronic Signature*) et PAdES (PDF *Advanced Electronic Signature*) définis par l'ETSI[1].

Ce produit est destiné à être utilisé, par des applications appelantes nécessitant la mise en œuvre d'un processus de signature électronique et/ou de vérification de signature, dans divers environnement d'exécution : applications autonomes, navigateurs Internet ou serveur d'application.

## 1.2. Description du produit

### *1.2.1. Introduction*

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

La cible de sécurité s'inspire des profils de protection [PP-ACSE-CCv3.1] et [PP-MVSE-CCv3.1].

### *1.2.2. Identification du produit*

La version du produit évaluée est 3.3.5.
Le numéro de version apparait :

- sur le support CD-ROM contenant le produit évalué ;
- dans le fichier MetaSIGN_version.iso présent sur le CD-ROM ;
- dans le fichier MANIFEST.MF présent sur le CD-ROM.

L'empreinte SHA1 suivante du fichier MetaSIGN_version.iso est également fournie dans le bon de livraison du produit :

5e8ea7481c4fe1f9d19799bced627c0f1c1f1614

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

[1] *European Telecommunications Standards Institute*.

### *1.2.3. Services de sécurité*

Les principaux services proposés par le produit sont :

- la génération d'une signature électronique d'un document ou de données, en utilisant un dispositif sécurisé de création de signature électronique[1] (module cryptographique hors périmètre d'évaluation) ;
- la vérification d'une signature électronique avec, optionnellement, l'augmentation de la signature. L'augmentation consiste à collecter et à signer les données de vérification (certificats d'Autorité de Certification, Liste de Certificats Révoqués, horodatage, etc.) qui seront utilisées lors des vérifications ultérieures.

### *1.2.4. Architecture*

Les modules constitutifs de la cible d'évaluation sont :

- un **module de génération de signature** électronique ;
- un **module de vérification** de la validité d'une signature électronique. Ce module permet également d'augmenter la signature de toutes les valeurs nécessaires aux vérifications ultérieures ;
- un **module de configuration** des différents paramètres qui seront utilisés lors de demandes de signature ou de vérification de signature ;
- un **module d'utilitaires** permettant d'accéder à différentes fonctions pour la gestion des magasins de politiques de signature, de certificats et de *CRLs.*

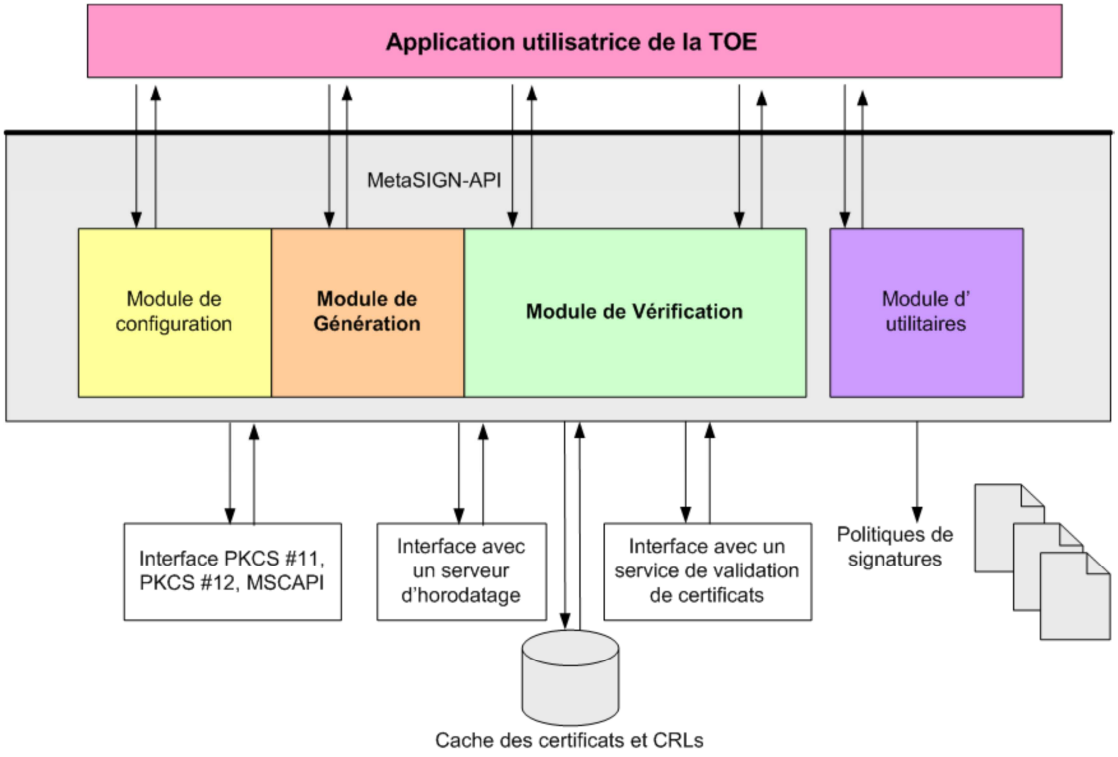


**Figure 1 - Architecture et périmètre de la TOE (*Target Of Evaluation*)**

[1] *SSCD : Secure Signature Creation Device.*

La cible d'évaluation (TOE) requiert les prérequis suivants pour être dans la configuration évaluée :

- un environnement d'exécution Java JRE SUN/ORACLE 6 mise à jour 31 ou supérieur ;
- un dispositif sécurisé de création de signature électronique ;
- des composants logiciels de communication avec le dispositif sécurisé de création de signature électronique ;
- une Infrastructure de Gestion de Clés de délivrance des certificats de signature ;
- un serveur d'horodatage permettant la délivrance des jetons d'horodatage.

La liste détaillée de la bibliothèque composant de la cible d'évaluation est décrite dans le §1.4.2 de la cible de sécurité [ST].

### *1.2.5. Cycle de vie*

Le cycle de vie du produit est le suivant :

1. la définition du besoin ;
2. la spécification et l'implémentation de la solution retenue ;
3. la validation de la solution ;
4. l'intégration de la solution sur les projets clients ;
5. la diffusion de la solution chez le client ;
6. la maintenance corrective ;
7. la gestion des versions.

L'évaluation a porté sur les étapes 1 à 3 du cycle de vie.

Le produit a été développé sur le site suivant :

*BULL SAS* (Groupe *ATOS*)

Rue Jean Jaurès
78340 Les Clayes sous-bois
France

La bibliothèque MetaSIGN-API est destinée à être intégrée dans des applications appelantes permettant de doter celles-ci des fonctions de création et/ou de vérification de signature électronique. Ainsi, pour l'évaluation, le développement des applications appelantes est considéré en tant que phase d'utilisation du produit au sens des [CC].

### *1.2.6. Configuration évaluée*

Le certificat de la bibliothèque MetaSIGN-API porte sur la configuration d'évaluation suivante :

- un poste client comprenant :
  - un système d'exploitation MICROSOFT Windows7 ;
  - un dispositif *SSCD* GEMALTO IDPrime MD 840 et sa librairie logicielle PKCS#11 associée ;
  - un navigateur Internet (Internet Explorer) version 11 ;
  - un environnement d'éxécution : *ORACLE* Java *Runtime Environment 7 update 67 ;*
  - des tests JAVA *« jUnit* » de validation de la cible d'évaluation ;
  - un environnement de développement Eclipse permettant d'exécuter les tests

JAVA « jUnit » Des pages HTML de tests permettant de télécharger les applets de génération et de vérification de signature ;

- un serveur comprenant :
  - une Infrastructure de Gestion de Clés permettant de délivrer des certificats de signature de test, produit *BULL* MetaPKI Version 9.5.8 ;
  - n serveur d'horodatage permettant de délivrer des jetons d'horodatage de test pour les signatures augmentées, produit *BULL* Version 9.5.8.

# 2. L'évaluation

## 2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs version 3.1 révision 3 [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

## 2.2. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 23 décembre 2015 détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

## 2.3. Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

La cotation des mécanismes cryptographiques a été réalisée conformément au référentiel technique de l'ANSSI [REF]. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY]. Les mécanismes analysés sont conformes aux exigences des référentiels cryptographiques de l'ANSSI. Les résultats ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau AVA_VAN.3 visé.

## 2.4. Analyse du générateur d'aléas

Le produit comporte un générateur d'aléas logiciel fournir en standard par la *Java Virtual Machine* (JVM) d'*ORACLE*. Celui-ci est utilisé pour la génération des clés de session du protocole TLS lors d'échanges avec des services extérieurs (ex : horodatage, récupération de politiques de signature, etc.).

Ce générateur d'aléas utilise la fonction de hachage SHA1 et la sortie du générateur peut être prédite par compromission de son état interne. Le générateur d'aléas n'est donc pas conforme aux exigences des référentiels cryptographiques de l'ANSSI.

Une précaution particulière doit être prise sur l'environnement d'exécution du générateur d'aléas afin de garantir que son état interne ne puisse être compromis.

# 3. La certification

## 3.1. Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

Ce certificat atteste que le produit « MetaSIGN-API » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 3 augmenté des composants ALC_FLR.3 et AVA_VAN.3.

## 3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du produit certifié doit s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment :

- les recommandations sur la configuration de MetaSIGN-API :
  - la signature des documents doit se faire uniquement grâce à l'utilisation d'une clé privée se trouvant dans un dispositif sécurisé de signature électronique *(SSCD)* certifié Critères Communs EAL4+ ;
  - les tailles de clés RSA pouvant être utilisées sont : 2048 bits et 4096 bits ;
  - les algorithmes de hachage pouvant être utilisés pour la signature RSA sont : SHA256, SHA384 et SHA512 ;
  - le signataire du ou des documents doit obligatoirement donner son consentement avant de procéder à la génération de la signature ;
  - les listes de révocation de certificats fournies par les Autorités de Certification et les contremarques de temps fournis par les horodateurs depuis un point de distribution distant doivent fournir des informations intègres ;
  - lorsque la communication avec un service externe est requise pour la récupération des documents à signer, des politiques de signature ou des listes de révocation de certificats, il est recommandé d'utiliser le protocole TLS ;
  - le mécanisme interne de vérification des certificats fourni par MetaSIGN-API doit être utilisé ;
  - les algorithmes de transformation XPATH et XSLT à appliquer sur les données à signer avant génération de la signature ne doivent pas être utilisés ;

- les recommandations sur l'application appelante de MetaSIGN-API :
  - l'application appelante doit utiliser le fichier MetaSIGN-API et les bibliothèques associées qui ont été signés par le certificat de *BULL* ;
  - l'application appelante doit posséder des applications de visualisation externe qui retranscrivent fidèlement le type de document à vérifier ou à signer et identifier les applications de présentation à exécuter ;

- l’environnement d’utilisation de MetaSIGN-API doit fournir à l’application appelante les moyens de contrôler l’intégrité des services et des paramètres de MetaSIGN-API ;
- l’application appelante doit s’assurer que toutes les données de validation sont disponibles ;
- l’application appelante doit s’assurer de l’authenticité de l’origine des politiques de signature avant qu’elles ne soient utilisées par MetaSIGN-API ;
- l'application appelante ne doit pas être utilisée ou exécutée en mode « administrateur » sur le poste de travail afin de garantir l'interdiction d'écriture et de lecture de fichiers sur les répertoires non accessibles par l'utilisateur de l'application ;

- les recommandations sur la machine hôte de MetaSIGN-API :
  - la machine hôte sur laquelle MetaSIGN-API s'exécute doit être sous la responsabilité d'une personne morale ou physique qui garantit l’application des mesures de sécurité ;
  - le système d'exploitation de la machine hôte doit offrir des contextes d'exécution séparés pour les différentes tâches qu'il exécute ;
  - la machine hôte doit être protégée contre les virus ;
  - les échanges entre la machine hôte et d'autres machines via un réseau ouvert doivent être contrôlés par un pare feu contrôlant et limitant les échanges ;
  - l'accès aux fonctions d'administration de la machine hôte doit être restreint aux seuls administrateurs de celle-ci ;
  - l'installation et la mise à jour de logiciels sur la machine hôte doit être sous le contrôle de l'administrateur ;
  - le système d'exploitation de la machine hôte doit refuser l'exécution d'applications téléchargées ne provenant pas de sources sûres.

## 3.3. Reconnaissance du certificat

### *3.3.1. Reconnaissance européenne (SOG-IS)*

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique jusqu'au niveau ITSEC E3 Elémentaire et CC EAL4. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

### *3.3.2. Reconnaissance internationale critères communs (CCRA)*

Ce certificat est émis dans les conditions de l'accord du CCRA [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[2], des certificats Critères Communs.
Pour les évaluations enregistrées avant septembre 2014, la reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL4 ainsi qu'à la famille ALC_FLR.
Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Autriche, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.
[2] Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, le Pakistan, les Pays-Bas, la République de Corée, la République Tchèque, le Royaume-Uni, la Suède et la Turquie.

# Annexe 1. Niveau d'évaluation du produit

| Classe | Famille | Composants par niveau d'assurance | | | | | | | Niveau d'assurance retenu pour le produit | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | EAL 1 | EAL 2 | EAL 3 | EAL 4 | EAL 5 | EAL 6 | EAL 7 | EAL 3+ | Intitulé du composant |
| **ADV Développement** | ADV_ARC | | **1** | 1 | 1 | 1 | 1 | 1 | **1** | Security architecture description |
| | ADV_FSP | **1** | **2** | **3** | **4** | **5** | 5 | **6** | **3** | Functional specification with complete summary |
| | ADV_IMP | | | | **1** | 1 | **2** | 2 | | |
| | ADV_INT | | | | | **2** | **3** | 3 | | |
| | ADV_SPM | | | | | | **1** | 1 | | |
| | ADV_TDS | | **1** | **2** | **3** | **4** | **5** | **6** | **2** | Architectural design |
| **AGD Guides d'utilisation** | AGD_OPE | **1** | 1 | 1 | 1 | 1 | 1 | 1 | **1** | Operational user guidance |
| | AGD_PRE | **1** | 1 | 1 | 1 | 1 | 1 | 1 | **1** | Preparative procedures |
| **ALC Support au cycle de vie** | ALC_CMC | **1** | **2** | **3** | **4** | 4 | **5** | 5 | **3** | Authorisation controls |
| | ALC_CMS | **1** | **2** | **3** | **4** | **5** | 5 | 5 | **3** | Implementation representation CM coverage |
| | ALC_DEL | | **1** | 1 | 1 | 1 | 1 | 1 | **1** | Delivery procedures |
| | ALC_DVS | | | **1** | 1 | 1 | **2** | 2 | **1** | Identification of security measures |
| | ALC_FLR | | | | | | | | **3** | Systematic flaw remediation |
| | ALC_LCD | | | **1** | 1 | 1 | 1 | **2** | **1** | Developer defined life-cycle model |
| | ALC_TAT | | | | **1** | **2** | **3** | 3 | | |
| **ASE Evaluation de la cible de sécurité** | ASE_CCL | **1** | 1 | 1 | 1 | 1 | 1 | 1 | **1** | Conformance claims |
| | ASE_ECD | **1** | 1 | 1 | 1 | 1 | 1 | 1 | **1** | Extended components definition |
| | ASE_INT | **1** | 1 | 1 | 1 | 1 | 1 | 1 | **1** | ST introduction |
| | ASE_OBJ | **1** | **2** | 2 | 2 | 2 | 2 | 2 | **2** | Security objectives |
| | ASE_REQ | **1** | **2** | 2 | 2 | 2 | 2 | 2 | **2** | Derived security requirements |
| | ASE_SPD | | **1** | 1 | 1 | 1 | 1 | 1 | **1** | Security problem definition |
| | ASE_TSS | **1** | 1 | 1 | 1 | 1 | 1 | 1 | **1** | TOE summary specification |
| **ATE Tests** | ATE_COV | | **1** | **2** | 2 | 2 | **3** | 3 | **2** | Analysis of coverage |
| | ATE_DPT | | | **1** | 1 | **3** | 3 | **4** | **1** | Testing: basic design |
| | ATE_FUN | | **1** | 1 | 1 | 1 | **2** | 2 | **1** | Functional testing |
| | ATE_IND | **1** | **2** | 2 | 2 | 2 | 2 | **3** | **2** | Independent testing: sample |
| **AVA Estimation des vulnérabilités** | AVA_VAN | **1** | **2** | 2 | **3** | **4** | **5** | 5 | **3** | Focused vulnerability analysis |

# Annexe 2. Références documentaires du produit évalué

| | |
|---|---|
| [ST] | Cible de sécurité de référence pour l'évaluation :<br>- Cible de sécurité METASIGN-API version 1.14, référence EVALCC-MSIGN-ST-01 du 30 novembre 2015, Bull. |
| [RTE] | Rapport technique d'évaluation :<br>- METASIGN-API v3.0, référence OPPIDA/CESTI/METASIGN-API/RTE/3.0 du 22 décembre 2015, OPPIDA. |
| [ANA-CRY] | Analyse des mécanismes cryptographiques :<br>- Evaluations MetaSIGN-API, MetaSIGN-APPLET, référence OPPIDA/CESTI/MetaSIGN/CRYPTO/2.2, OPPIDA. |
| [CONF] | Liste de configuration du produit :<br>- Liste de configuration, référence metasignConfig_1.5 version 1.5, Bull. |
| [GUIDES] | Guides d'utilisation du produit :<br>- Guide général de programmation version 1.12, référence MSIGN-API-GDE-01 du 27 août 2015, Bull ;<br>- Guide de programmation pour le signature CAdES version 1.4, référence MSIGN-API-GDE-21 du 9 mars 2015, Bull ;<br>- Guide de programmation pour le signature PAdES version 1.4, référence MSIGN-API-GDE-31 du 9 mars 2015, Bull ;<br>- Guide de programmation pour la signature XAdES version 2.13, référence MSIGN-API-GDE-11 du 12 octobre 2015, Bull ;<br>- Description des interfaces version 2.15, référence MSIGN-API-INT-11 du 12 octobre 2015, Bull ;<br>- Guide des codes de retours de MetaSIGN version 1.6, référence MSIGN-API-GDE-04 du 18 septembre 2015, Bull ;<br>- Configuration des paramètres version 1.28, référence MSIGN-API-GDE-02 du 18 septembre 2015, Bull ;<br>- Description des politiques de signature au format XML version 1.14 référence MSIGN-PS-02 du 7 septembre 2015, Bull ;<br>- Description du rapport de vérification version 2.6, référence MSIGN-API-GDE-03 du 16 juillet 2015, Bull. |
| [PP-ACSE-CCv3.1] | Profil de Protection, Application de Création de Signature Electronique, version 1.7, 2 mars 2011.<br>*Certifié par l'ANSSI sous la référence ANSSI-CC-PP-2008/05-M01 le 21 mars 2011.* |
| [PP-MVSE-CCv3.1] | Profil de Protection, Module de Vérification de Signature Electronique, version 1.7, du 2 mars 2011.<br>*Certifié par l'ANSSI sous la référence ANSSI-CC-PP-2008/06-M01 le 21 mars 2011.* |

# Annexe 3. Références liées à la certification

| | |
|---|---|
| Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information. | |
| [CER/P/01] | Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, ANSSI. |
| [CC] | Common Criteria for Information Technology Security Evaluation :<br>Part 1: Introduction and general model,<br>juillet 2009, version 3.1, révision 3 Final, référence CCMB-2009-07-001;<br>Part 2: Security functional components,<br>juillet 2009, version 3.1, révision 3 Final, référence CCMB-2009-07-002;<br>Part 3: Security assurance components,<br>juillet 2009, version 3.1, révision 3 Final, référence CCMB-2009-07-003. |
| [CEM] | Common Methodology for Information Technology Security Evaluation : Evaluation Methodology,<br>juillet 2009, version 3.1, révision 3 Final, référence CCMB-2009-07-004. |
| [REF] | Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr. |
| [CC RA] | Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, 2 juillet 2014. |
| [SOG-IS] | « Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 janvier 2010, Management Committee. |