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*

Paris, le 14 JUIN 2016
N° 2340 /ANSSI/SDE/PSS/BQA

QUALIFICATION AU NIVEAU STANDARD

METASIGN version 3.3.5
(composé des éléments METASIGN-APPLET version 3.3.5 et METASIGN-API version 3.3.5)

BULL SAS (GROUPE ATOS)

Annexes : 1. Conditions de validité de la qualification.
2. Base documentaire.

Le produit METASIGN version 3.3.5 est destiné à mettre en œuvre la signature électronique et la vérification de signature dans des applications Web utilisatrices à travers deux composantes : une interface programmatique via l'applet METASIGN-API, et des services de signature et de vérification de signature dans les navigateurs internet via l'applet METASIGN-APPLET. L'accès à ces services pour une application se fait donc via l'interface programmatique METASIGN-API.

Sur la base des cibles de sécurité en référence [6] et [7] et des rapports de certification en référence [8] et [9], et sous réserve des restrictions et recommandations en annexe 1, j'atteste que le produit METASIGN version 3.3.5 atteint le niveau de qualification standard conformément au processus de qualification en référence [1].

De plus, l'évaluation a montré que le produit est conforme au profil de protection *« Application de Création de Signature Électronique »* en référence [4] et *«Module de Vérification de Signature Électronique »* en référence [5], et qu'il répond donc aux exigences des niveaux ** et *** du RGS, en référence [2] applicables aux dispositifs de signature.

En outre, ce produit est déclaré apte à satisfaire les exigences du règlement européen sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, dit règlement eIDAS [3] et peut ainsi être mis en œuvre dans le cadre de la signature avancée ou qualifiée.

Cette qualification est valable pour une durée de 3 ans. Elle pourra être prolongée par la mise sous surveillance des produits certifiés METASIGN-API et METASIGN-APPLET, et est assujettie au maintien en condition opérationnelle (MCO) et de sécurité (MCS) de la solution sur la durée de la qualification. De plus, cette qualification est conditionnée à l'existence d'une configuration logicielle compatible avec le produit (*a minima*, système d'exploitation, navigateur et *plugin* Java) et bénéficiant d'un maintien en condition de sécurité actif par les éditeurs concernés.

Contre-amiral Dominique RIBAN
Directeur général adjoint

Annexe 1

Conditions de validité de la qualification

1 Restrictions sur l'environnement d'exploitation de METASIGN

[R1]. L'utilisateur du produit doit s'assurer de la conformité de l'environnement d'exécution, tel que spécifié dans la cible de sécurité. Pour rappel, la configuration évaluée du poste hôte est la suivante :

- un système d'exploitation *MICROSOFT* Windows7 ;
- un navigateur Internet « Internet Explorer » version 11 ;
- un environnement d'exécution : *ORACLE* Java Runtime Environment 7 update 67.

[R2]. L'utilisateur du produit doit s'assurer du maintien en condition de sécurité (MCS) de l'ensemble des composants de l'environnement d'exécution nécessaire au produit, système d'exploitation, navigateur, environnement Java et *plugin* de navigateur associé.

2 Conditions sur le maintien en condition opérationnelle (MCO) et de sécurité (MCS)

[R3]. Le développeur du produit doit sur la durée de la qualification assurer un suivi de sécurité et un maintien en condition opérationnelle (MCO) et de sécurité (MCS) du produit vis-à-vis des vulnérabilités du système d'exploitation, du navigateur Internet et de l'environnement d'exécution.

3 Conditions sur la configuration de METASIGN

[R4]. 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 augmenté de AVA_VAN.5[1].

[R5]. Les tailles de clés RSA pouvant être utilisées sont 2048 bits et 4096 bits.

[R6]. Les algorithmes de hachage pouvant être utilisés pour la signature RSA sont SHA256, SHA384 et SHA512.

[R7]. Le signataire du ou des documents doit obligatoirement donner son consentement avant de procéder à la génération de la signature.

[R8]. Les listes de révocation de certificats fournies par les Autorités de Certification et les contremarques de temps fournies par les horodateurs depuis un point de distribution distant doivent fournir des informations intègres.

[R9]. 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.

[R10]. Le mécanisme interne de vérification des certificats fourni par METASIGN-APPLET doit être utilisé.

---

[1] Conforme au profil de protection n°BSI-CC-PP-0059-MA-01.

[R11]. Les algorithmes de transformation XPATH et XSLT à appliquer sur les données à signer avant génération de la signature ne doivent pas être utilisés.

[R12]. *[spécifique à METASIGN-APPLET]* Pour chaque document à signer, l'application utilisatrice doit configurer METASIGN-APPLET pour lui permettre d'interroger un module externe chargé d'identifier si la sémantique du document est bien stable.

[R13]. *[spécifique à METASIGN-APPLET]* La configuration de METASIGN-APPLET ne doit pas permettre la signature d'un document si elle ne peut déterminer quelle application de visualisation lancer. La prise en charge de la visualisation des fichiers au format texte (.txt) est native au produit. Pour tous les autres cas, le module externe d'affichage du document doit être 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 Conditions sur l'application Web utilisatrice de METASIGN

[R14]. L'application Web utilisatrice doit utiliser le fichier METASIGN et les bibliothèques associées qui ont été signés par le certificat de *BULL*.

[R15]. L'application Web utilisatrice 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.

[R16]. L'environnement d'utilisation de METASIGN doit fournir à l'application Web utilisatrice les moyens de contrôler l'intégrité des services et des paramètres de METASIGN.

[R17]. L'application Web utilisatrice doit s'assurer que toutes les données de validation sont disponibles.

[R18]. L'application Web utilisatrice doit s'assurer de l'authenticité de l'origine des politiques de signature avant qu'elles ne soient utilisées par METASIGN.

[R19]. L'application Web utilisatrice 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.

[R20]. *[spécifique à METASIGN-APPLET]* L'application Web utilisatrice, lors d'une vérification de signature, ne doit pas utiliser la méthode permettant de renseigner les données signées lorsque la signature contient une référence aux données signées. Les données signées seront extraites depuis la référence incluse dans la signature.

5 Conditions sur la machine hôte de METASIGN

[R21]. La machine hôte sur laquelle METASIGN s'exécute doit être sous la responsabilité d'une personne morale ou physique qui garantit l'application des mesures de sécurité.

[R22]. Le système d'exploitation de la machine hôte doit offrir des contextes d'exécution séparés pour les différentes tâches qu'il exécute.

[R23]. La machine hôte doit être protégée contre les virus.

[R24]. 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.

[R25]. L'accès aux fonctions d'administration de la machine hôte doit être restreint aux seuls administrateurs de celle-ci.

[R26]. L'installation et la mise à jour de logiciels sur la machine hôte doit être sous le contrôle de l'administrateur.

[R27]. Le système d'exploitation de la machine hôte doit refuser l'exécution d'applications téléchargées ne provenant pas de sources sûres.

Annexe 2

Base documentaire

1. Processus de qualification d'un produit de sécurité - niveau standard -, version 1.2, disponible sur www.ssi.gouv.fr.
2. Référentiel général de sécurité, versions 1.0 et 2.0.
3. Règlement européen n°910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive n°1999/93/CE.
4. Profil de protection « Application de création de signature électronique - PP-ACSE-CCv3.1, version 1.7», réf. ANSSI-CC-PP-2008/05-M01 du 2 mars 2011.
5. Profil de protection « Module de vérification de signature électronique - PP-MVSE-CCv3.1, version 1.7 », réf. ANSSI-CC-PP-2008/06-M01 du 2 mars 2011.
6. Cible de sécurité MetaSIGN-API version 1.14, réf. n° EVALCC-MSIGN-ST-01 du 30 novembre 2015.
7. Cible de sécurité MetaSIGN-Applet version 1.14, réf. n° EVALCC-MSIGN-ST-02 du 30 novembre 2015.
8. Rapport de certification, réf. n°ANSSI-CC-2016/10 du 25/03/2016.
9. Rapport de certification, réf. n°ANSSI-CC-2016/09 du 21/03/2016.