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 30 mai 2011

N° 1419/ANSSI/SR

Référence : ANSSI-CC-NOTE-15/1.0

NOTE D'APPLICATION

SIGNATURE PRESUMEE FIABLE ET SECURE MESSAGING

DANS LE CADRE DES CARTES A MICROPROCESSEUR

Application : Dès son approbation.

Diffusion : Publique.

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

Patrick PAILLOUX

Suivi des modifications

Edition	Date	Modifications
1.0	30 mai 2011	Première édition officielle.

La présente instruction est disponible en ligne sur les sites suivants :

- le site institutionnel de l'ANSSI (www.ssi.gouv.fr) ;
- le site institutionnel du SGDSN (www.sgdsn.gouv.fr) ;
- le site prévu par le décret n° 2008-1281 du 8 décembre 2008 pour la publication des instructions et circulaires (www.circulaires.gouv.fr).

TABLE DES MATIERES

1 Objet de la note

La présente note expose la position de l'ANSSI sur la nécessité d'utiliser un *Secure Messaging* entre le dispositif sécurisé de création de signature (SSCD, *Secure Signature Creation Device*), considéré ici comme étant une carte à microprocesseur, et l'application de création de signature (SCA, *Signature Creation Application*), dans le contexte de la signature présumée fiable telle que définie dans le décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique.

2 Documents de référence

- [BSI-PP-0005-2002] Protection profile – Secure Signature-Creation Device Type 2, Version 1.04 ;
- [BSI-PP-0006-2002] Protection profile – Secure Signature-Creation Device Type 3, Version 1.05 ;
- [DCSSI-PP-2008/05] Profil de protection « Application de création de signature électronique », référence : PP-ACSE-CCv3.1, version 1.6 ;
- [DCSSI-PP-2008/06] Profil de protection « Module de vérification de signature électronique », référence : PP-MVSE-CCv3.1, version 1.6.

3 Présentation de la situation

Les profils de protection certifiés par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) sous les références [BSI-PP-0005-2002] et [BSI-PP-0006-2002] précisent qu'un canal de confiance doit pouvoir être établi entre le SSCD et le SCA pour la communication des éléments à signer et pour les résultats fournis par la carte (voir l'exigence FTP_ITC dans les PP cités). Avec les cartes à puce, ce canal de confiance est normalement établi en mettant en œuvre la fonctionnalité de *Secure Messaging*[1]. Les SSCD conformes aux profils de protection [BSI-PP-0005-2002] et [BSI-PP-0006-2002] doivent donc proposer ce mécanisme.

Toutefois, l'ANSSI considère que, selon le contexte d'utilisation du SSCD, l'usage du *Secure Messaging* est optionnel, y compris dans le cadre de la signature présumée fiable. Le paragraphe ci-dessous précise ces différents contextes.

4 Cas d'utilisation du Secure Messaging

4.1 Cas d'un environnement d'utilisation supposé de confiance entre le SSCD et le SCA

Un cas typique de mise en œuvre de la signature électronique est l'utilisation d'un poste de travail sur lequel s'exécute une application de création (ou de vérification) de signature auquel est directement connecté un SSCD via un dispositif assurant l'interface de communication (typiquement, un lecteur de carte). D'autres configurations matérielles peuvent être envisagées. Le point important est que les communications entre le SSCD et l'application de création (ou de vérification) de signature sont supposées avoir le même niveau de confiance que le poste de travail.

Dans ce cas, l'utilisation d'un *Secure Messaging* pour réaliser le canal de confiance est optionnel. Le fait de ne pas utiliser le *Secure Messaging* ne remet pas en cause la présomption de fiabilité de la signature.

[1] Le *Secure Messaging* permet d'assurer l'authentification mutuelle, l'intégrité et l'authenticité des données et éventuellement, leur chiffrement.

Justification : L'établissement d'un *Secure Messaging* suppose que le poste de travail mémorise des clés cryptographiques pour permettre l'authentification et le dialogue chiffré entre l'application de création (ou de vérification) de signature et le SSCD. Or, pour que la signature soit considérée comme valide, le poste de travail doit être considéré comme étant dans un environnement de confiance. C'est en particulier ce qui est préconisé dans les profils de protection [DCSSI-PP-2008/05] et [DCSSI-PP-2008/06] concernant les applications de création et de vérification de signature (voir par exemple, H.Machine_Hôte dans ces profils de protection).

Si l'environnement permet d'atteindre ce niveau de confiance, l'usage du *Secure Messaging* n'apporte rien en termes de sécurité (que ce soit pour l'échange de DTBS (*Data to be signed*), du VAD (*Verification authentication data*) ou du RAD (*Reference authentication data*)). En revanche, il peut compliquer considérablement la mise en œuvre de la signature électronique en termes de gestion des clés.

Cette approche est d'ailleurs confirmée par les nouveaux profils de protection SSCD (en CC V3.1) en cours de vote au CEN (comité européen de normalisation), dans lesquels deux catégories sont distinguées : signature en environnement de confiance et signature dans un environnement qui n'est pas de confiance.

4.2 Autres cas

Si la liaison entre le SSCD et le poste de travail hébergeant le SCA n'est pas sûr, il est nécessaire d'utiliser le *Secure Messaging*.