Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PRIME MINISTER

*Secrétariat général*
*de la défense*
*et de la sécurité nationale*

*Agence nationale de la sécurité*
*des systèmes d'information*

Paris, 30 mai 2011

N° 1419/ANSSI/SR

Reference: ANSSI-CC-NOTE-15/1.0ENEN

# APPLICATION NOTE

## QUALIFIED SIGNATURE AND SECURE MESSAGING IN THE CONTEXT OF MICROPROCESSOR CARDS

| | | |
|---|---|---|
| Application | : | From date of publication. |
| Circulation | : | Public. |

**COURTESY TRANSLATION**

SÉCURITÉ CERTIFICATION

# Version history

| Version | Date | Modification |
|---|---|---|
| 1.0 | 30 May 2011 | First official edition. |

This instruction is available online at the following sites:

- The ANSSI institutional site (www.ssi.gouv.fr);
- The SGDSN institutional site (www.sgdsn.gouv.fr);
- The site specified in decree No. 2008-1281 of 8th December 2008 for the publication of instructions and circulars (www.circulaires.gouv.fr).

# TABLE OF CONTENTS

# 1 Subject of the note

This note outlines the ANSSI's position on the need to use *Secure Messaging* between the *Secure Signature Creation Device* (SSCD), which in this case is considered to be a microprocessor board, and the *Signature Creation Application* (SCA) in the context of the qualified signature as defined in decree No. 2001-272 of 30th March 2001 taken for application of article 1316-4 of the civil code relating to electronic signature.

# 2 Reference documents

- [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 », reference: PP-ACSE-CCv3.1, version 1.6;
- [DCSSI-PP-2008/06] Profil de protection « Module de vérification de signature électronique », reference: PP-MVSE-CCv3.1, version 1.6.

# 3 Presentation of the situation

The protection profiles certified by the BSI (*Bundesamt für Sicherheit in der Informationstechnik*) under references [BSI-PP-0005-2002] and [BSI-PP-0006-2002] specify that a trusted channel must be established between the SSCD and the SCA to communicate elements to be signed and for the results provided by the board (see requirement FTP_ITC in the PP quoted). With smart cards, this trusted channel is normally established by implementing the *Secure Messaging*[1] functionality. The SSCD that are compliant with protection profiles [BSI-PP-0005-2002] and [BSI-PP-0006-2002] must therefore propose this mechanism.

However, the ANSSI considers that depending on how the SSCD is used, the use of *Secure Messaging* is optional, including in the context of the qualified signature. The section below specifies these different contexts.

# 4 Secure Messaging usage scenario

## 4.1 Case of a supposed trusted environment between the SSCD and the SCA

A typical case where the electronic signature is implemented is the use of a workstation where a signature creation (or verification) application is used, to which an SSCD is connected directly to provide the communication interface (typically a card reader). Other hardware configurations are possible. The important point is that the communications between the SSCD and the signature creation (or verification) application are supposed to have the same level of trust as the workstation.

In this case, *Secure Messaging* for the trusted channel is optional. The presumed reliability of the signature is not called into question if *Secure Messaging* is not used.

**Justification**: The establishment of *Secure Messaging* supposes that the workstation stores cryptographic keys to enable the authentication and encrypted dialogue between the signature creation (or verification) application and the SSCD. However, for the signature to be considered as valid, the workstation must be considered as being in a trusted environment. This is what is recommended in particular in the protection profiles [DCSSI-

[1] *Secure Messaging* ensures the mutual authentication, integrity and authenticity of the data and where applicable its encryption.

PP-2008/05] and [DCSSI-PP-2008/06] concerning the signature creation and verification applications (for example, see H.Machine_Hôte in these protection profiles).

If the environment enables this level of trust to be reached, *Secure Messaging* provides nothing in terms of security (whether for the exchange of DTBS (*Data to be signed*), VAD (*Verification authentication data*) or RAD (*Reference authentication data*)). However, it may complicate considerably the implementation of the electronic signature in terms of key management.

In addition, this approach is confirmed by the new SSCD protection profiles (in CC V3.1) which are currently being voted on at the CEN (European Committee for Standardisation), in which two categories are distinguished: signature in a trusted environment and signature in an environment which is not trusted.

## 4.2 Other cases

*Secure Messaging* must be used if the link between the SSCD and the SCA host workstation is not secure.