Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
nationale

*Direction centrale de la sécurité des systèmes d'information*

Paris, le 24 octobre 2005.

N°3033/SGDN/DCSSI/SDR
Référence : PSC/P/01.1

# PROCEDURE

## CERTIFICATION DE CONFORMITE DES MODULES CRYPTOGRAPHIQUES DES PSC

Objet : Certification de conformité des modules cryptographiques des PSC

Application :

Diffusion : Public

| Vérifié par | Validé par<br><br>Le sous- directeur de la régulation | Après consultation des membres du comité directeur<br>Approuvé par<br>Le directeur central de la sécurité des systèmes d'information |
|---|---|---|
| *Le responsable qualité*<br>Thomas Bousson<br>[ORIGINAL SIGNE]<br>*Le chef du centre de certification*<br>Pascal Chour<br>[ORIGINAL SIGNE] | Pascal Chauve<br>[ORIGINAL SIGNE] | Patrick Pailloux<br>[ORIGINAL SIGNE] |

# Suivi des modifications

| Révisions | Dates | Modifications |
|---|---|---|
| 1 | 18/12/03 | Création du document. |
| 2 | 06/10/05 | Compléments apportés au document suite à l'avis du comité directeur de la certification et de l'adoption de l'arrêté du 26 juillet 2004. |
| | | |
| | | |

# TABLE DES MATIERES

**1. OBJET DE LA PROCEDURE ..... 4**

**2. LE CONTEXTE ..... 4**

2.1. LE CONTEXTE JURIDIQUE ..... 4
2.2. LES DEUX NIVEAUX DE RECONNAISSANCE DE LA SIGNATURE ELECTRONIQUE ..... 4
2.3. LE CONTEXTE EUROPEEN ..... 5

**3. LA PROCEDURE D'ATTRIBUTION DU CERTIFICAT DE CONFORMITE ..... 5**

3.1. EXIGENCES SUR LE MODULE CRYPTOGRAPHIQUE DU PSC ..... 5
3.2. INSERTION DANS LE SCHEMA FRANÇAIS DE CERTIFICATION ..... 6
3.3. FORME DU CERTIFICAT DE CONFORMITE ..... 6
3.4. CONDITIONS DE DELIVRANCE DU CERTIFICAT DE CONFORMITE ..... 6
3.5. EXIGENCES SUR LES AUTRES PROFILS DE PROTECTION OU CIBLES DE SECURITE SOUMISES ..... 6
3.6. ORGANISMES DELIVRANT LE CERTIFICAT DE CONFORMITE ..... 6
3.7. VALIDITE DU CERTIFICAT DE CONFORMITE ..... 7

**4. RECOMMANDATIONS DE LA DCSSI ..... 7**

4.1. RECOMMANDATIONS DE PROFILS DE PROTECTION ..... 7
4.2. RECOMMANDATIONS D'ALGORITHMES CRYPTOGRAPHIQUES ..... 7
4.3. RECOMMANDATIONS SUR LA SURVEILLANCE DU MODULE CRYPTOGRAPHIQUE ..... 7
4.4. UTILISATION D'AUTRES STANDARDS DE CERTIFICATION ..... 7

# 1. Objet de la procédure

Cette procédure s'adresse aux fournisseurs de modules cryptographiques utilisés par des prestataires de services de certification pour la génération de certificats qualifiés.

Le certificat de conformité délivré suivant cette procédure atteste que le module cryptographique respecte l'ensemble des exigences du point 2 de l'annexe de l'arrêté du 26 juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation.

Ce certificat de conformité est requis pour tout prestataire souhaitant être qualifié suivant les règles définies dans l'arrêté du 26 juillet 2004.

# 2. Le contexte

## 2.1. Le contexte juridique

La directive européenne du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques a été transposée essentiellement dans la loi n°2000-230 du 13 mars 2000 et dans le décret d'application n°2001-272 du 30 mars 2001.

La loi n°2000-230 définit deux niveaux de reconnaissance juridique pour une signature électronique, présentés au §2.2 :

- la signature électronique « simple »,
- la signature électronique « présumée fiable ».

Le décret n°2001-272 énonce les conditions requises pour qu'un procédé de signature électronique soit présumé fiable. L'une de ces conditions est que la vérification de la signature repose sur l'utilisation d'un certificat électronique qualifié. Un certificat électronique est reconnu comme qualifié s'il comporte les éléments énumérés à l'article 6.I de ce même décret et s'il est délivré par un prestataire de services de certification (PSC) satisfaisant aux exigences fixées à l'article 6.II du décret.

## 2.2. Les deux niveaux de reconnaissance de la signature électronique

### 2.2.1. La signature électronique « simple »

L'article 4 de la loi n°2000-230 du 13 mars 2000 définit la signature électronique en ces termes :

*« Lorsqu'elle [la signature] est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. »*

A ce niveau, le procédé de signature électronique n'est pas présumé fiable mais l'écrit signé ainsi sous forme électronique ne pourra être refusé en justice au titre de preuve dès lors que le procédé permet d'identifier le signataire et de garantir le lien avec l'acte signé. En cas de contestation, il appartient au signataire de prouver la fiabilité du procédé de signature électronique utilisé.

### 2.2.2. La signature électronique présumée fiable

L'article 4 de la loi n°2000-230 du 13 mars 2000 précise que la charge de la preuve peut être inversée, en cas de contestation, sous certaines conditions définies par décret :

*« La fiabilité de ce procédé est présumée, jusqu'à preuve du contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées en Conseil d'Etat. »*

L'article 2 du décret du 30 mars 2001 décrit les conditions suivant lesquelles le procédé de signature électronique est considéré comme fiable :

- la signature électronique est sécurisée,
- la signature électronique est établie grâce à un dispositif sécurisé de création de signature,

- la vérification de la signature électronique repose sur l'utilisation d'un certificat électronique qualifié.

Seule la condition énoncée au troisième point est traitée dans cette procédure. La condition énoncée au deuxième point fait l'objet de la procédure SIG-P-01.

Le décret n°2001-272 énonce qu'un certificat électronique délivré par un prestataire de services de certification qualifié est présumé qualifié. L'arrêté du 26 juillet 2004 fixe les règles techniques selon lesquelles un PSC est évalué en vue d'une qualification, précisant ainsi l'article 6 du décret n°2001-272. Parmi ces règles, figurent, au point 2 de l'annexe de l'arrêté, des exigences qui s'appliquent au module cryptographique du PSC et dont le respect se traduit par la délivrance d'un certificat de conformité.

L'objet de ce document est de décrire la procédure d'attribution de ce certificat de conformité qui incombe à la DCSSI.

## 2.3. Le contexte européen

La DCSSI se base sur les travaux de l'EESSI (European Electronic Signature Standardization Initiative), initiative européenne de normalisation qui a été lancée par la Commission européenne à la suite de la directive européenne 1999/93/CE. L'EESSI a produit de nombreux documents et la DCSSI en a retenu certains.

Conformément à la Directive 1999/93/CE, la Commission européenne a publié le 15 juillet 2003 au journal officiel de l'Union européenne une décision en date du 14 juillet 2003 référençant des normes, après consultation du Comité article 9 instauré par la directive et composé de représentants des Etats membres. Les modules cryptographiques conformes aux normes référencées (CWA 14167-1 et CWA 14167-2) sont présumés conformes aux exigences du point f de l'annexe 2 de la directive.

# 3. La procédure d'attribution du certificat de conformité

## 3.1. Exigences sur le module cryptographique du PSC

Le point 2 de l'annexe de l'arrêté du 26 juillet 2004 fixe les exigences que doit satisfaire le module cryptographique du PSC :

*«*

- *assurer la confidentialité et l'intégrité des données de création de signature du prestataire de services de certification durant tout leur cycle de vie ;*
- *être capable d'identifier et d'authentifier ses utilisateurs ;*
- *limiter l'accès à ses services en fonction de l'utilisateur et du rôle qui lui a été assigné ;*
- *être capable de mener une série de tests pour vérifier qu'il fonctionne correctement et entrer dans un état sûr s'il détecte une erreur ;*
- *détecter les tentatives d'altérations physiques et entrer dans un état sûr quand une tentative d'altération est détectée ;*
- *permettre de créer une signature électronique sécurisée, pour signer les certificats, qui ne révèle pas les données de création de signature du prestataire de services de certification et qui ne peut pas être falsifiée sans la connaissance des données de création de signature du prestataire de services de certification ;*
- *créer des enregistrements d'audit pour chaque modification concernant la sécurité ;*
- *si une fonction de sauvegarde et de restauration des données de création de signature du prestataire de services de certification électronique est offerte, garantir la confidentialité et l'intégrité des données sauvegardées et réclamer au minimum un double contrôle des opérations de sauvegarde et de restauration. »*

Les exigences énumérées ci-dessus seront désignées, dans la suite du document, par le terme « exigences de l'arrêté ».

Par ailleurs, si le prestataire de services de certification génère les données de création et de vérification de signature du signataire, destinées à un dispositif sécurisé de création de signature, le module cryptographique utilisé doit être certifié, pour cette fonction, conforme aux exigences définies à l'article 3.I du décret n°2001-272, tel que spécifié dans la procédure SIG-P-01.

## 3.2. Insertion dans le schéma français de certification

En se plaçant dans le cadre du décret n°2002-535 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, l'évaluation du produit à certifier doit avoir lieu dans un centre d'évaluation agréé par la DCSSI. Ces centres d'évaluation réalisent des évaluations suivant des critères normalisés : les ITSEC ou les « Critères Communs » (CC). L'évaluation permet de s'assurer de la conformité d'un produit à une cible de sécurité, laquelle peut être conforme à un profil de protection.

L'évaluation, préalable à la délivrance d'un certificat de conformité à l'arrêté, doit s'appuyer sur une cible de sécurité qui couvre complètement les exigences de l'arrêté et dont le niveau d'assurance est acceptable en fonction de l'environnement choisi.

## 3.3. Forme du certificat de conformité

Le certificat de conformité délivré par la DCSSI prend la forme d'un document distinct complémentaire du certificat CC ou ITSEC délivré pour le produit lui-même.

Le certificat de conformité portera mention du rapport de certification relatif au certificat CC ou ITSEC sur lequel il s'appuie.

## 3.4. Conditions de délivrance du certificat de conformité

Deux cas peuvent se présenter lors de l'évaluation du module :

- la cible de sécurité, élaborée par le commanditaire de l'évaluation, est conforme à l'un des profils de protection recommandés par la DCSSI (cf. §4). Dans ce cas, la cible de sécurité est présumée conforme aux exigences de l'arrêté et le certificat de conformité peut être attribué après évaluation et certification du module suivant cette cible de sécurité ;
- le commanditaire peut proposer une cible de sécurité qui n'est pas conforme à l'un des profils de protection recommandés par la DCSSI. Dans ce cas, il doit prouver que la cible proposée répond aux exigences de l'arrêté. La DCSSI attribue le certificat de conformité lorsque cette preuve est apportée d'une part et que le module est certifié suivant cette cible de sécurité d'autre part.

De plus, le certificat de conformité à l'arrêté n'est délivré qu'après acceptation par la DCSSI des algorithmes utilisés. L'analyse des mécanismes cryptographiques est obligatoire et est effectuée par la DCSSI.

Si le module a fait l'objet d'un certificat CC ou ITSEC délivré par un autre pays, la DCSSI se réserve le droit de réaliser une analyse des mécanismes cryptographiques utilisés avant de délivrer le certificat de conformité.

## 3.5. Exigences sur les autres profils de protection ou cibles de sécurité soumises

Dans le cas où le commanditaire proposerait une cible non conforme à l'un des profils de protection recommandés par la DCSSI (cf. §4), la cible de sécurité proposée doit respecter des exigences minimales :

- les objectifs de sécurité de la cible doivent couvrir les exigences de l'arrêté ;
- les exigences d'assurance de la cible de sécurité doivent correspondre au niveau EAL 4 + pour une évaluation selon les CC. Le niveau EAL 4 doit être augmenté par au moins le composant d'assurance AVA_VLA.4. Dans le cas d'une évaluation selon les ITSEC, le niveau d'assurance devra être « E3 high ».

## 3.6. Organismes délivrant le certificat de conformité

L'arrêté du 26 juillet 2004 spécifie les conditions suivant lesquelles le module cryptographique du PSC est certifié conforme aux exigences de l'arrêté en ces termes :

*« Le module cryptographique utilisé par le prestataire de services de certification électronique pour les fonctions assurées doit, dans les conditions prévues par le décret n°2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, être certifié conforme par le Premier ministre aux exigences ci-après»*

Le décret n°2002-535 désigne la DCSSI.

### 3.7. Validité du certificat de conformité

En cas de fait porté à la connaissance de la DCSSI et qui remet en cause la conformité du module aux exigences du l'arrêté, le certificat de conformité est révoqué.

## 4. Recommandations de la DCSSI

### 4.1. Recommandations de profils de protection

La DCSSI recommande de recourir à l'un des profils de protection (PP) suivants :

- le PP CMCSOB (CWA 14167-2) si une fonction de sauvegarde et de restauration des données de création de signature du PSC est offerte ;
- le PP CMCSO (CWA 14167-4) si aucune fonction de sauvegarde et de restauration des données de création de signature du PSC n'est offerte.

### 4.2. Recommandations d'algorithmes cryptographiques

La DCSSI recommande l'utilisation du document de la DCSSI sur les règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard (DCSSI_ALGO).

La conformité à ce guide ne présume pas de l'acceptation par la DCSSI des mécanismes cryptographiques implémentés dans le module.

### 4.3. Recommandations sur la surveillance du module cryptographique

Le certificat de conformité à l'arrêté est lié au certificat CC ou ITSEC qui donne, entre autres, un niveau d'assurance sur la capacité du module cryptographique à atteindre les objectifs définis dans sa cible de sécurité. Les attaques évoluant, un produit certifié peut devenir vulnérable aux nouvelles attaques de l'état de l'art apparues depuis sa certification CC ou ITSEC. Dans ces conditions, la conformité aux exigences de l'arrêté pourrait être contestée s'il était démontré que le produit ne résiste pas à une ou plusieurs attaques de l'état de l'art.

Afin de prévenir ce risque ou tout au moins, de permettre de le gérer, la DCSSI recommande de mettre le module cryptographique sous processus de surveillance tel que défini dans SUR-P-01. Ce processus permet, par l'intermédiaire d'analyses de vulnérabilités régulières, de s'assurer de la robustesse du produit face à l'évolution de l'état de l'art des attaques.

### 4.4. Utilisation d'autres standards de certification

La DCSSI examine au cas par cas toute autre preuve de certification du module considéré, ne résultant pas d'une évaluation suivant les CC ou les ITSEC, et se réserve le droit d'exiger tout document nécessaire à cette étude (certificat, rapport de certification, rapport d'évaluation, cible de sécurité…) en vue de la délivrance du certificat de conformité.

D'autre part, tout litige ou toute contestation concernant l'attribution du certificat de conformité à l'arrêté est porté à la connaissance du comité directeur de la certification.

# Annexe A Abréviations

| | |
|---|---|
| **CC** | Critères Communs / Common Criteria |
| **DCSSI** | Direction Centrale de la Sécurité des Systèmes d'Information |
| **ITSEC** | Information Technology Security Evaluation Criteria |
| **CMCSO** | Cryptographic Module for CSP Signing Operation |
| **PSC** | Prestataire de Services de Certification |

# Annexe B Références


**Directive 1999/93/CE** du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques.
http://www.ssi.gouv.fr/fr/reglementation/loi_europe/1999_93_CE.pdf

**Décision de la Commission du 14 juillet 2003** relative à la publication des numéros de référence de normes généralement admises pour les produits de signatures électroniques conformément à la directive 1999/93/CE du Parlement européen et du Conseil.
http://www.ssi.gouv.fr/fr/reglementation/loi_europe/l_175.pdf

**Loi n°2000-230 du 13 mars 2000** portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.
http://www.ssi.gouv.fr/fr/reglementation/loi2000-230.pdf

**Décret n°2001-272 du 30 mars 2001** pris pour application de l'art 1316-4 du code civil et relatif à la signature électronique, modifié par l'article 20 du décret 2002-535.
http://www.ssi.gouv.fr/fr/reglementation/decret2001-272.html

**Décret n°2002-535 du 18 avril 2002** relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.
http://www.ssi.gouv.fr/fr/reglementation/decret2002-535.html

**Arrêté du 26 juillet 2004** relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation.
http://www.ssi.gouv.fr/fr/reglementation/arr26072004.pdf

**CC** Common Criteria for Information Technology Security Evaluation
http://www.ssi.gouv.fr/fr/confiance/methodologie.html

**CWA 14167-1** European Committee for Standardization CEN/ISS: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1: System Security Requirements.
ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14167-01-2003-Jun.pdf

**CWA 14167-2** European Committee for Standardization CEN/ISS: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 2: Cryptographic module for CSP signing operations with backup – Protection profile CMCSOB-PP.
ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14167-02-2004-May.pdf

**CWA 14167-4** European Committee for Standardization CEN/ISS: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 4: Cryptographic module for CSP signing operations with backup – Protection profile CMCSO-PP.
ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14167-04-2004-May.pdf

**DCSSI_ALGO** Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard, DCSSI, version 1.02 du 19 novembre 2004.
http://www.ssi.gouv.fr/site_documents/politiqueproduit/Mecanismes_cryptographique_v1_02_standard.pdf

**ITSEC** Critères d'évaluation de la sécurité des systèmes informatiques (ITSEC), version 1.2, juin 1991.

http://www.ssi.gouv.fr/site_documents/ITSEC/ITSEC-fr.pdf

**SIG-P-01** Procédure de certification de conformité des dispositifs de création de signature électronique, DCSSI, version 01.1 du 7 avril 2003.

http://www.ssi.gouv.fr/site_documents/certification/SIG-P-01_Certif_de_conformite_des_DCS_elec.pdf

**SUR-P-01** Procédure de surveillance des produits certifiés, DCSSI, version 01.1 du 9 février 2004.

http://www.ssi.gouv.fr/site_documents/certification/SUR-P-01_Surveillance_des_produits_certifies.pdf