Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
nationale

Direction centrale de la sécurité des systèmes d'information

Paris, le 7 avril 2003

872 /SGDN/DCSSI/SDR
Référence : SIG/P/01.1

PROCEDURE

CERTIFICATION DE CONFORMITE DES DISPOSITIFS DE CREATION DE SIGNATURE ELECTRONIQUE

Objet : Certification de conformité des dispositifs de création de signature électronique
Application : A compter du 7 avril 2003
Diffusion : Publique

Vérifié par	Validé par Le sous-directeur "Régulation"	Vu l'avis du comité directeur Approuvé par Le Directeur central de la sécurité des systèmes d'information
Le responsable qualité ORIGINAL SIGNE *Le chef du centre de certification* ORIGINAL SIGNE	ORIGINAL SIGNE	ORIGINAL SIGNE

Suivi des modifications

Révisions	Dates	Modifications
1	7/04/2003	Vu l'avis du comité directeur de la certification

TABLE DES MATIERES

1. OBJET DE LA PROCEDURE 4

2. LE CONTEXTE 4

2.1. Le contexte juridique 4
2.2. Les deux niveaux pour la signature électronique 4
2.2.1. La signature électronique « simple » 4
2.2.2. La signature électronique présumée fiable 4
2.3. Le contexte européen 5

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

3.1. Exigences sur le dispositif sécurisé de création de signature électronique 5
3.2. Insertion dans le schéma français de certification 5
3.3. Forme du certificat de conformité 6
3.4. Conditions de délivrance du certificat de conformité 6
3.5. Organismes délivrant le certificat de conformité 6
3.6. Validité du certificat de conformité 6

4. RECOMMANDATIONS DE LA DCSSI 7

4.1. Recommandations de profils de protection 7
4.2. Recommandations d'algorithmes cryptographiques 7
4.3. Exigences sur les autres profils de protection ou cibles de sécurité soumises 7
4.4. Utilisation d'autres standards de certification 7

ANNEXE A TABLEAU DES PROFILS DE PROTECTION RECOMMANDES 9

ANNEXE B ABREVIATIONS 10

ANNEXE C REFERENCES 11

1. Objet de la procédure

Cette procédure définit la procédure de délivrance d'un certificat de conformité aux exigences de l'article 3.I du décret 2001-272 du 30 mars 2001, relatif à la signature électronique, pour un dispositif sécurisé de création de signature électronique.

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 dans la loi 2000-230 du 13 mars 2000 et dans le décret d'application 2001-272 du 30 mars 2001.

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

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

Le décret 2001-272 pose les conditions requises pour qu'une signature électronique soit présumée fiable. L'une de ces conditions est que le dispositif sécurisé de création de signature (SSCD) soit certifié conforme aux exigences de la directive européenne prévues dans son annexe III et reprises dans l'art 3.I du décret 2001-272.

2.2. Les deux niveaux pour la signature électronique

2.2.1. La signature électronique « simple »

L'article 4 de la loi 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 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 selon 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 deuxième tiret est traitée dans cette procédure.

Pour qu'un dispositif de création de signature soit reconnu comme sécurisé, il doit répondre à un certain nombre d'exigences décrites dans l'art. 3.I du décret 2001-272 (cf. § 3.1) et être certifié conforme à ces exigences.

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 devrait publier au JOCE des normes, après consultation du Comité article 9 (instauré par la Directive et composé de représentants des Etats membres). Les dispositifs certifiés conformes aux normes référencées seront présumés conformes aux exigences de la Directive. Cependant, à l'heure actuelle, la Commission européenne n'a publié aucune décision dans ce domaine.

Conformément à l'article 3.II.2 du décret 2001-272 (transposition de l'article 3.4 de la Directive européenne), ce certificat de conformité est reconnu dans chacun des Etats membres.

3. La procédure d'attribution du certificat de conformité

3.1. Exigences sur le dispositif sécurisé de création de signature électronique

L'article 3.I du décret 2001-272 fixe les exigences que doit satisfaire un dispositif sécurisé de création de signature électronique, ainsi :

« Un dispositif sécurisé de création de signature électronique doit :

1. *Garantir par des moyens techniques et des procédures appropriés que les données de création de signature électronique :*
    a. *ne peuvent être établies plus d'une fois et que leur confidentialité est assurée :*
    b. *ne peuvent être trouvées par déduction et que la signature électronique est protégée contre toute falsification ;*
    c. *peuvent être protégées de manière satisfaisante par le signataire contre toute utilisation par des tiers.*
2. *N'entraîner aucune altération du contenu à signer et ne pas faire obstacle à ce que le signataire en ait une connaissance exacte avant de le signer. »*

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

Est considéré comme faisant partie du SSCD, le module permettant de créer les données de création et de vérification de signature électronique et de générer la signature électronique. Nous excluons ainsi du périmètre du SSCD l'application pilotant le module cité, le système d'exploitation sur lequel l'application est installée ainsi que l'ensemble des dispositifs se trouvant dans l'environnement du SSCD. En revanche, le canal de transmission entre le SSCD et l'application de signature électronique doit être sûr, c'est à dire que l'intégrité des données à signer transmises par l'application au SSCD est exigée sauf si le SSCD se trouve dans un environnement protégé (chez le prestataire de service). Cette exigence n'est vérifiée lors de l'évaluation du SSCD que lorsque celui-ci est amené à être utilisé en environnement ouvert (chez l'utilisateur final).

3.2. Insertion dans le schéma français de certification

En se plaçant dans le cadre du décret 2002-535, l'évaluation du dispositif 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 (de moins en moins utilisés) ou la norme ISO/IEC 15408 (aussi appelée « Critères Communs » (CC)). L'évaluation permet de certifier la conformité d'un dispositif à une cible de sécurité qui peut être conforme à un profil de protection.

L'évaluation, préalable à la délivrance d'un certificat de conformité au décret, doit s'appuyer sur une cible de sécurité qui couvre complètement les exigences du décret 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 des fonctions pour lesquelles il a été délivré et du rapport de certification relatif au certificat CC ou ITSEC sur lequel il s'appuie.

Si le commanditaire ne fait évaluer qu'une partie du dispositif (fonction de génération de données de création de signature électronique ou fonction de création de signature électronique), il se verra attribuer un certificat de conformité portant mention de la fonction couverte par le dispositif. L'utilisation du dispositif devra se faire conjointement avec un autre dispositif ayant également obtenu un certificat de conformité portant mention de la fonction complémentaire.

3.4. Conditions de délivrance du certificat de conformité

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

- la cible de sécurité, élaborée par le commanditaire de l'évaluation, est conforme à l'un des profils de protection recommandés par la DCSSI. Dans ce cas, la cible de sécurité est présumée conforme aux exigences du décret et le certificat de conformité peut être attribué après évaluation et certification du dispositif 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 répond aux exigences du décret 2001-272. La DCSSI attribue le certificat de conformité lorsque cette preuve est apportée d'une part et que le dispositif est certifié suivant cette cible de sécurité d'autre part.

De plus, le certificat de conformité au décret n'est délivré qu'après acceptation par la DCSSI des algorithmes utilisés. L'analyse cryptographique est obligatoire et est effectuée par la DCSSI suivant une note d'application du schéma sur la cryptologie.

Si le dispositif a fait l'objet d'un certificat de conformité CC ou ITSEC délivré par un autre pays, la DCSSI se réserve le droit d'examiner les algorithmes utilisés avant de délivrer le certificat de conformité au décret 2001-272.

3.5. Organismes délivrant le certificat de conformité

L'art. 3.II du décret 2001-272 spécifie les conditions suivant lesquelles le dispositif de création de signature électronique est certifié conforme aux exigences du décret en ces termes :

« Un dispositif sécurisé de création de signature électronique doit être certifié conforme aux exigences définies au I :

1. *Soit par le Premier ministre, 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. La délivrance du certificat de conformité est rendue publique ;*
2. *Soit par un organisme désigné à cet effet par un Etat membre de la Communauté européenne. »*

Le décret 2002-535 désigne la DCSSI.

3.6. Validité du certificat de conformité

Le certificat de conformité au décret est lié au certificat CC ou ITSEC. Or l'état de l'art des attaques, pour lesquels le certificat CC ou ITSEC a été délivré, peut évoluer rapidement.

De ce fait, le certificat CC ou ITSEC, qui a permis l'attribution du certificat de conformité, doit rentrer dans un processus de surveillance, défini dans une procédure du schéma de certification. La DCSSI a donc la possibilité de demander, à tout moment, une évaluation supplémentaire du dispositif si elle estime que l'état de l'art a changé de manière significative.

En cas d'échec au processus de surveillance ou par tout autre fait porté à la connaissance de la DCSSI et qui remet en cause la conformité du dispositif aux exigences du décret, le certificat de conformité est révoqué.

4. Recommandations de la DCSSI

4.1. Recommandations de profils de protection

La DCSSI recommande des profils de protection, reportés dans le tableau en annexe A, en prenant en compte l'environnement dans lequel la cible est utilisée et les fonctions pour lesquels ils ont été écrits.

Il existe en effet deux types d'environnement :

- l'environnement de l'utilisateur final,
- l'environnement du prestataire de service de certification (PSC).

D'autre part, un dispositif sécurisé de création de signature électronique complet doit assurer au minimum les fonctions suivantes :

- la génération des données de création (clé secrète) et de vérification (clé publique) de signature électronique,
- la création de la signature électronique.

Chacune de ces fonctions peut être réalisée par un module distinct et faire l'objet d'un certificat de conformité (cf. § 3.3).

4.2. Recommandations d'algorithmes cryptographiques

La DCSSI encourage l'utilisation du document produit par l'EESSI sur les algorithmes recommandés pour la signature électronique « Algorithms and Parameters for Secure Electronic Signatures ». Il s'agit d'un guide qui :

- liste les algorithmes existant acceptables pour la signature électronique et la taille minimale des clés à utiliser pour ces algorithmes,
- prévoit le temps de validité des algorithmes recommandés.

Pour chaque demande de certificat de conformité au décret, une analyse cryptographique est demandée par la DCSSI (cf. § 3.4) et devra atteindre le niveau de cotation « élevé ».

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

Dans le cas où le commanditaire propose une cible non conforme à l'un des profils de protection recommandés par la DCSSI, celle-ci doit respecter des exigences minimales :

- les objectifs de sécurité de la cible doivent couvrir les exigences du décret,
- les exigences d'assurance de la cible de sécurité doivent correspondre au niveau EAL 4 +.

En fonction de l'environnement dans lequel se trouve le SSCD évalué, les composants d'assurance augmentant le niveau EAL 4 exigés sont au minimum :

- en milieu ouvert : AVA_MSU.3 , AVA_VLA.4,
- en milieu protégé : ADV_IMP.2, AVA_CCA.1, AVA_VLA.4.

Dans le cas d'une évaluation selon les ITSEC, le niveau d'assurance devra être « E3 high » et les composants d'assurance requis devront être examinés au cas par cas en coopération entre le commanditaire de l'évaluation et la DCSSI.

4.4. Utilisation d'autres standards de certification

Si le dispositif considéré a déjà fait l'objet d'une certification selon un standard autre que les ITSEC ou les CC, la DCSSI étudie au cas par cas les évaluations supplémentaires nécessaires à la délivrance du certificat de conformité et le commanditaire doit délivrer à la DCSSI l'ensemble des documents nécessaires à cette étude, comme le rapport d'évaluation.

La DCSSI étudie au cas par cas les situations non couvertes par cette procédure.

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

Annexe A Tableau des profils de protection recommandés

Profil de protection retenu	**N° de norme EESSI**	**Environnement considéré**	**Fonction de génération des données de création et de vérification de signature électronique (1)**	**Fonction de création de signature électronique (2)**	**Conformité au décret 2001-272 (art. 3.I)**
PP SSCD type1 Secure Signature Creation Device type 1	CWA 14169 Annexe A	Utilisateur	Oui	Non	Conformité pour la fonction (1)
PP SSCD type 2 Secure Signature Creation Device type 2	CWA 14169 Annexe B	Utilisateur	Non	Oui	Conformité pour la fonction (2)
PP SSCD type 3 Secure Signature Creation Device type 3	CWA 14169 Annexe C	Utilisateur	Oui	Oui	Conformité
PP MCSO Cryptographic Module for CSP Signing Operation	CWA 14167-2	Prestataire de service de certification	Oui	Oui	Conformité
PP CMCKG Cryptographic Module for CSP Key Generation Services	CWA 14167-3 (à paraître)	Prestataire de service de certification	Oui	Non	Conformité pour la fonction (1)

Annexe B Abréviations

CC	Critères Communs / Common Criteria
CEM	Common Evaluation Methodology / Méthode d'Evaluation Commune
CMCKG	Cryptographic Module for CSP Key Generation Services
COFRAC	Comité Français d'Accréditation
DCSSI	Direction Centrale de la Sécurité des Systèmes d'Information
IT	Instruction Technique
ITSEC	Information Technology Security Evaluation Criteria
ITSEM	Information Technology Security Evaluation Methodology
MCSO	Module for CSP Signing Operation
PSC / CSP	Prestataire de Service de Certification / Certification Service Provider
SSCD	Secure Signature Creation Device / Dispositif sécurisé de création de signature

Annexe C Références

Directive 1999/93/CE	du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques.
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.
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.
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
CWA 14169	European Committee for Standardization CEN/ISS : Security Requirements of Secure Signature Creation Devices (SSCD) – SSCD-PP
CWA 14167-2	European Committee for Standardization CEN/ISS : Security Requirements of Cryptographic Module for CSP Signing Operations – MCSO-PP
CWA 14167-3	European Committee for Standardization CEN/ISS : Security Requirements of Cryptographic Module for CSP Key Generation Services – CMCKG-PP
ITSEC	Critères d'évaluation de la sécurité des systèmes informatiques (ITSEC), version 1.2, juin 1991.
ISO/IEC 15408	Information technology — Security techniques — Evaluation criteria for IT security : ISO/IEC 15408-1:1999(E) : Part 1 : Introduction and general model ; ISO/IEC 15408-2:1999(E) : Part 2 : Security functional requirements ; ISO/IEC 15408-3:1999(E) : Part 3 : Security assurance requirements.
CC	Common Criteria for Information Technology Security Evaluation : Part 1 : Introduction and general model, version 2.1, août 1999 ; Part 2 : Security functional requirements, version 2.1, août 1999 ; Part 3 : Security assurance requirements, version 2.1, août 1999.