Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Premier ministre

Agence nationale de la sécurité des systèmes d'information

Dispositifs de création de signature / cachet électronique qualifiés

Certification de la conformité au règlement eIDAS

Version 1.0 du 16 novembre 2017

HISTORIQUE DES VERSIONS			
DATE	**VERSION**	**EVOLUTION DU DOCUMENT**	**REDACTEUR**
20/06/2016	0.9	*Version de travail pour commentaires*	ANSSI
16/11/2017	1.0	Version pour application au 16 novembre 2017. *Modifications :* - *Ajout des modalités de contact de l'ANSSI* - *Précisions sur la maintenance de la certification* - *Définition des engagements du commanditaire de la certification*	ANSSI

Les commentaires sur le présent document sont à adresser à :

Agence nationale de la sécurité des systèmes d'information

SGDSN/ANSSI

51 boulevard de La Tour-Maubourg
75700 Paris 07 SP

supervision-eIDAS@ssi.gouv.fr

SOMMAIRE

I. Introduction

I.1. Objet

L'objet de ce document est de décrire la procédure d'attribution par l'ANSSI des certificats de conformité pour les dispositifs de création de signature et électronique qualifiés (DCSQ[1]) au sens de l'article 30 du règlement [eIDAS] et de cachet électronique qualifié (DCCQ[2]) au sens de l'article 39 du règlement [eIDAS].

Le règlement prévoit que pour créer une signature électronique ou un cachet électronique dits « qualifiés », les dispositifs de création de signature électronique et de création de cachet électronique doivent eux-mêmes être qualifiés. Les exigences applicables à ces dispositifs sont exprimées dans l'annexe II du règlement [eIDAS].

La conformité de ces dispositifs aux exigences du règlement [eIDAS] est certifiée nationalement par un organisme certificateur. En France, l'ANSSI a été désignée comme organisme certificateur par la note des autorités françaises [DESIGNATION].

Les chapitres qui suivent précisent les conditions d'obtention d'un certificat de conformité pour un DCSQ / DCCQ.

L'annexe 2 donne un exemple d'implémentation d'un DCSQ ou DCCQ lorsque les données de création de signature ou de cachet électronique sont gérées par un PSCo qualifié pour le compte de l'utilisateur.

Ce document abroge la procédure SIG/P/01.1, référence 872/SGDN/DCSSI/SDR du 7 avril 2003.

I.2. Cadre juridique

Les dispositifs de création de signature / cachet électronique qualifiés, certifiés conformément à la présente procédure, et figurant dans la liste publiée par la Commission européenne, sont présumés satisfaire aux exigences de l'annexe II du règlement [eIDAS].

Les signatures électroniques avancées, reposant sur un certificat qualifié de signature électronique, et créées à l'aide d'un dispositif de création de signature électronique qualifié, sont des signatures électroniques qualifiées, bénéficiant des effets juridiques prévus à l'article 25 du règlement [eIDAS] et à l'article 1367 du Code civil des Français.

Les cachets électroniques avancés, reposant sur un certificat qualifié de cachet électronique, et créés à l'aide d'un dispositif de création de cachet électronique qualifié, sont des cachets électroniques qualifiés, bénéficiant des effets juridiques prévus à l'article 35 du règlement [eIDAS].

I.3. Mise à jour

L'opportunité de la mise à jour de ce document est évaluée par l'ANSSI et peut notamment être le fait d'une évolution du cadre réglementaire ou normatif lié au règlement [eIDAS] ou d'une évolution de l'état de l'art.

L'ANSSI précise la date d'effet de chaque mise à jour et les modalités de transition le cas échéant.

---

1 « *Qualified electronic Signature Creation Device* » (QSCD) en anglais.

2 « *Qualified electronic Seal Creation Device* » (QSCD) en anglais.

I.4. Acronymes

Les acronymes utilisés dans le présent document sont les suivants :

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information.
CC	Critères Communs / *Common Criteria*.
DCCQ	Dispositif de Création de Cachet électronique Qualifié
DCSQ	Dispositif de Création de Signature électronique Qualifiée.
DSCS	Dispositif Sécurisé de Création de Signature électronique.
HSM	*Hardware Security Module*. Voir RCM.
PSCo	Prestataire de service de confiance
QSCD	*Qualified electronic Signature Creation Device* ou *Qualified electronic Seal Creation Device*. Voir DCSQ ou DCCQ.
RCM	Ressource Cryptographique Matérielle. Enceinte sécurisée en mesure de protéger l'intégrité et la confidentialité de secrets et de réaliser des calculs cryptographiques en toute sécurité.
SSCD	*Secure Signature Creation Device.* Cf. directive européenne 1999/93/CE abrogée par le règlement [eIDAS]. Voir DSCS.
SOG-IS	*Senior Officials Group-Information System Security.* Accord européen pour la reconnaissance des certificats de sécurité (notamment CC). Voir www.sogis.org.

II. Exigences relatives aux dispositifs de création de signature / cachet électronique qualifiés

II.1. Processus d'attribution du certificat de conformité

II.1.1. Demande du certificat de conformité

La demande de certificat de conformité est adressée au Bureau Qualification et Agrément de l'ANSSI (qualification@ssi.gouv.fr). Cette demande doit être accompagnée des éléments sur lesquels repose la décision de certification de conformité (par exemple, le rapport de certification du dispositif selon les Critères Communs).

Le bureau Politique Industrielle et Assistance de l'ANSSI (industries@ssi.gouv.fr) est le point de contact privilégié pour toute question relative à la démarche de certification de conformité d'un nouveau dispositif.

II.1.2. Forme du certificat de conformité

Le certificat de conformité délivré par l'ANSSI s'appuie sur un processus distinct et complémentaire du certificat de sécurité délivré pour le produit lui-même.

Le certificat de conformité porte mention des fonctions pour lesquelles il a été délivré et du rapport de certification relatif au certificat de sécurité sur lequel il s'appuie. Ce certificat de conformité peut comporter des restrictions d'usage qui doivent impérativement être respectées, notamment dans le cadre de la préparation, de la délivrance puis de la mise en œuvre du dispositif.

Dans le cas de la certification de conformité de DCSQ ou DCCQ utilisés dans l'environnement d'un prestataire de services de confiance qualifié, assurant la génération et la gestion des données de création de signature (respectivement de cachet) pour le compte du signataire (respectivement du créateur de cachet), un certificat de conformité partiel peut être délivré pour le seul produit. Ce certificat de conformité devra être complété après la vérification des modalités de mise en œuvre du DCSQ ou du DCCQ dans l'environnement d'un prestataire de services de confiance qualifié.

II.1.3. Validité du certificat de conformité

Le certificat de conformité est lié au certificat de sécurité initial, typiquement le certificat [CC]. Or l'état de l'art des attaques, en fonction duquel le certificat de sécurité a été délivré, peut évoluer.

De ce fait, le certificat de sécurité, qui a permis l'attribution du certificat de conformité, doit rentrer dans un processus de surveillance, tel que défini dans la note [CERTIF_SURV]. Le certificat de surveillance est attendu par l'ANSSI dans un délai maximal de 5 ans après la décision de certification [CC] ou la dernière surveillance.

En cas d'échec du processus de surveillance ou par tout autre fait porté à la connaissance de l'ANSSI et remettant en cause la conformité du dispositif aux exigences du règlement [eIDAS], l'ANSSI analyse au cas par cas le maintien (avec éventuellement des réserves d'emploi) ou la révocation du certificat de conformité. En particulier, le non-respect des engagements relatifs au suivi de sécurité du produit, détaillés en annexe 2 du présent document, est une cause de révocation du certificat de conformité.

Dans tous les cas, un certificat de conformité est automatiquement révoqué au bout d'une durée précisée dans le chapitre II.3 du présent document, selon le type de DCSQ ou DCCQ ayant fait l'objet de la certification de conformité.

II.2. Critères d'évaluation de la conformité des DCSQ et DCCQ

Les produits permettant la signature électronique qualifiée et le cachet électronique qualifié sont définis ainsi par le règlement [eIDAS], article 3 :

- « « **dispositif de création de signature électronique** », un dispositif logiciel ou matériel configuré servant à créer une signature électronique » ;
- « « **dispositif de création de signature électronique qualifié** », un dispositif de création de signature électronique qui satisfait aux exigences énoncées à l'annexe II » ;
- « « **dispositif de création de cachet électronique** », un dispositif logiciel ou matériel configuré utilisé pour créer un cachet électronique » ;
- « « **dispositif de création de cachet électronique qualifié** », un dispositif de création de cachet électronique qui satisfait mutatis mutandis aux exigences énoncées à l'annexe II ».

L'évaluation doit permettre de démontrer le respect des exigences applicables du règlement [eIDAS] telles que précisées dans son annexe II « **Exigences applicables aux dispositifs de création de signature électronique qualifiés** » :

1) Les dispositifs de création de signature électronique qualifiés garantissent au moins, par des moyens techniques et des procédures appropriés, que :
   a) la confidentialité des données de création de signature électronique utilisées pour créer la signature électronique est suffisamment assurée ;
   b) les données de création de signature électronique utilisées pour créer la signature électronique ne peuvent être pratiquement établies qu'une seule fois ;
   c) l'on peut avoir l'assurance suffisante que les données de création de signature électronique utilisées pour créer la signature électronique ne peuvent être trouvées par déduction et que la signature électronique est protégée de manière fiable contre toute falsification par les moyens techniques actuellement disponibles ;
   d) les données de création de signature électronique utilisées pour créer la signature électronique peuvent être protégées de manière fiable par le signataire légitime contre leur utilisation par d'autres.
2) Les dispositifs de création de signature électronique qualifiés ne modifient pas les données à signer et n'empêchent pas la présentation de ces données au signataire avant la signature.
3) La génération ou la gestion de données de création de signature électronique pour le compte du signataire peut être seulement confiée à un prestataire de services de confiance qualifié.
4) Sans préjudice du paragraphe 1, point d), un prestataire de services de confiance qualifié gérant des données de création de signature électronique pour le compte d'un signataire ne peut reproduire les données de création de signature électronique qu'à des fins de sauvegarde, sous réserve du respect des exigences suivantes :
   a) le niveau de sécurité des ensembles de données reproduits doit être équivalent à celui des ensembles de données d'origine ;
   b) le nombre d'ensembles de données reproduits n'excède pas le minimum nécessaire pour assurer la continuité du service.

Les exigences de cette annexe II s'appliquent, *mutatis mutandis*, aux dispositifs de création de cachet électronique qualifiés.

La certification de conformité à ces exigences est réalisée conformément à la décision d'exécution n°2016/650 [eIDAS_DE_QSCD] [3].

Pour les DCSQ ou DCCQ pour lesquels les données de création de signature ou de cachet électronique sont conservées dans un environnement sous le contrôle total de l'utilisateur, la certification de conformité repose sur les normes référencées dans l'annexe I de la décision d'exécution, dont les modalités d'application sont définies dans le présent document, paragraphe II.3.1.

Pour les DCSQ ou DCCQ pour lesquels les données de création de signature ou de cachet électronique sont gérées par un prestataire de services de confiance qualifié pour le compte du signataire ou du créateur de cachet, la certification de conformité repose sur un processus alternatif prévu par l'article 30.3.b du règlement [eIDAS]. Le présent document, paragraphe II.3.2, présente le processus mis en œuvre par l'ANSSI.

II.3. Modalités de certification de la conformité des DCSQ et DCCQ

II.3.1. Lorsque les données de création de signature ou de cachet électronique sont conservées dans un environnement sous le contrôle total de l'utilisateur

a. Délivrance du certificat de conformité

Le certificat de conformité du DCSQ ou DCCQ est délivré s'il est vérifié, par l'ANSSI en tant qu'organisme certificateur national, que :

- le système ou le produit dans lequel est mis en œuvre la clé privée de signature ou de cachet a été certifié dans le cadre de l'accord européen de reconnaissance mutuelle du SOG-IS[4] sur la base de l'un des profils de protection référencés dans la décision [eIDAS_DE_QSCD] ;

et

- la cryptographie répond aux règles définies dans le document [SOGIS-CRYPTO]. Cette vérification repose sur une analyse théorique des mécanismes cryptographiques et sur une expertise de leur implémentation.

Le certificat de conformité est délivré pour une version identifiée du DCSQ ou DCCQ, et la durée de validité du certificat de conformité est fixée dans la décision de certification. La durée de validité du certificat de conformité ne peut excéder 10 ans au-delà de la certification [CC] ou de la dernière surveillance du DCSQ/DCCQ.

La délivrance d'un certificat de conformité par l'ANSSI donne lieu à une notification à la Commission européenne, pour inscription dans la liste des DCSQ/DCCQ certifiés prévue à l'article 31 du règlement [eIDAS].

b. Maintenance du certificat de conformité

Toute nouvelle version doit faire l'objet d'une décision explicite d'extension du certificat de conformité, dans les mêmes conditions que la décision initiale d'attribution du certificat de conformité.

Une fois la décision de certification de conformité arrivée à échéance ou révoquée, le DCCQ/DCSQ est retiré de la liste publiée par la Commission européenne.

---

[3] voir http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016D0650

[4] voir http://www.ssi.gouv.fr/entreprise/produits-certifies/

II.3.2. Lorsque les données de création de signature ou de cachet électronique sont gérées par un PSCo qualifié pour le compte de l'utilisateur

a. Délivrance du certificat de conformité

Le certificat de conformité partiel du produit est délivré s'il est vérifié, par l'ANSSI en tant qu'organisme certificateur national, que :

- Le système ou le produit dans lequel est mis en œuvre la clé privée de signature ou de cachet a été certifié dans le cadre de l'accord européen de reconnaissance mutuelle du SOG-IS [4] sur la base d'une cible de sécurité validée par l'ANSSI[5] ;

et

- Les systèmes ou les produits concourant à protéger cette clé privée contre une utilisation par d'autres que le signataire ou le créateur de cachet légitime, ont été certifiés conformément à une stratégie définie préalablement avec l'ANSSI[6].

et

- la cryptographie répond aux règles définies dans le document [SOGIS-CRYPTO]. Cette vérification repose sur une analyse théorique des mécanismes cryptographiques et sur une expertise de leur implémentation.

L'annexe 3 du présent document donne un exemple d'implémentation permettant de répondre à ces exigences.

La délivrance d'un certificat de conformité partiel ne donne pas lieu à une notification à la Commission européenne pour inscription sur la liste des DCCQ/DCSQ certifiés prévue à l'article 31 du règlement [eIDAS]. L'ANSSI publie sur son site Internet la liste des certificats de conformité partiels délivrés.

Le certificat de conformité complet du DCSQ ou DCCQ est délivré si il est vérifié, par l'ANSSI en tant qu'organe de contrôle national, en application de l'article 20.2 du règlement [eIDAS], que :

- le système ou le produit est mis en œuvre dans l'environnement d'un prestataire de services de confiance qualifié, figurant dans la liste de confiance de l'un des Etats membres de l'Union européenne ;

et

- ce prestataire de services de confiance qualifié met en œuvre le produit ou le système conformément aux restrictions d'usage figurant dans son rapport de certification [CC] ;

et

- ce prestataire de services de confiance qualifié respecte les exigences formulées au point 4 de l'annexe II du règlement eIDAS ;

---

[5] En l'absence de profil de protection applicable à ces systèmes ou produits, il est nécessaire de rédiger une « cible de sécurité » (au sens [CC] du terme). Cette cible devra être analysée par l'ANSSI qui pourra déterminer si le système ou le produit répond bien aux exigences de l'annexe II du règlement et si le niveau de certification et les composants d'assurance retenus sont bien identiques à ceux demandés dans les profils de protection référencés dans la décision [eIDAS_DE_QSCD].

[6] L'annexe 2 présente un exemple de solution permettant la création de signature ou de cachet à distance, pour le compte de l'utilisateur, et précise dans ce cas de figure quels sont les composants devant faire l'objet d'une certification, et le niveau de certification nécessaire

et

- ce prestataire de services de confiance qualifié respecte les exigences du règlement applicables à l'ensemble des prestataires de services de confiance, précisées à l'article 5, de l'article 15, l'article 19, et en particulier dispose d'une analyse de risques à jour couvrant la mise en œuvre du produit ou système au sein de son environnement ;

et

- ce prestataire de services de confiance qualifié respecte les exigences du règlement applicables aux prestataires de services de confiance qualifiés, précisées dans la note [PSCO_QUALIF], sur l'environnement de mise en œuvre du DCSQ ou du DCCQ.

L'ANSSI peut déléguer tout ou partie des travaux d'évaluation de la conformité à ces exigences à un organisme d'évaluation de la conformité répondant aux critères de la note [CRITERES_OEC].

Le certificat de conformité est délivré pour une version identifiée de chaque système ou produit composant le DCSQ ou DCCQ, et la durée de validité du certificat de conformité est fixée dans la décision de certification. La durée de validité du certificat de conformité ne peut excéder 5 ans au-delà de la certification [CC] ou de la dernière surveillance du système ou produit dans lequel est mis en œuvre la clé privée de signature ou de cachet.

La délivrance d'un certificat de conformité complet par l'ANSSI donne lieu à une notification à la Commission européenne, pour inscription dans la liste des DCSQ/DCCQ certifiés prévue à l'article 31 du règlement [eIDAS]. Le certificat de conformité complet précise le nom du prestataire de services de confiance qualifié devant mettre en œuvre le DCSQ/DCCQ, et indique en restriction d'usage que la certification n'est valide que si le DCSQ/DCCQ est effectivement mis en œuvre par ce prestataire.

b. Maintenance du certificat de conformité

Toute nouvelle version du système ou produit dans lequel est mis en œuvre la clé privée de signature ou de cachet doit faire l'objet d'une décision explicite d'extension du certificat de conformité, dans les mêmes conditions que la décision initiale d'attribution du certificat de conformité.

Les nouvelles versions des systèmes ou produits concourant à protéger cette clé privée contre une utilisation par d'autres que le signataire ou le créateur de cachet légitime bénéficient implicitement de l'extension du certificat de conformité, sous réserve que :

1. Préalablement au déploiement de cette nouvelle version, soit adressée à l'ANSSI une analyse d'impacts recensant l'ensemble des modifications effectuées, la raison de ces modifications, et leur impact sur la sécurité ; et que

2. En parallèle du déploiement de cette nouvelle version, le fournisseur du dispositif :
    - apporte, dans un délai maximal de deux mois, des réponses à toute demande d'information complémentaire de l'ANSSI ; et
    - initie, dans un délai maximal de deux mois, tous travaux d'évaluation complémentaire demandés par l'ANSSI.

Une fois la décision de certification de conformité arrivée à échéance ou révoquée, le DCSQ/DCCQ est retiré de la liste publiée par la Commission européenne.

Annexes

I. Annexe 1 - Références documentaires

Renvoi	Document
[eIDAS]	Règlement n° 910/2014 du 23 juillet 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. Disponible sur http://www.europa.eu
[DESIGNATION]	Note des autorités française du 29 avril 2016 à la Commission, désignant l'ANSSI comme organisme certificateur au titre des articles 30 et 39 du règlement eIDAS.
[eIDAS_DE_QSCD]	Décision d'exécution (UE) n° 2016/650 de la commission du 25 avril 2016 établissant des normes relatives à l'évaluation de la sécurité des dispositifs qualifiés de création de signature électronique et de cachet électronique conformément à l'article 30, paragraphe 3, et à l'article 39, paragraphe 2, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur
[CC]	ISO/IEC 15408:2005 Common Criteria for Information Technology Security Evaluation : Part 1 : Introduction and general model; Part 2 : Security functional requirements; Part 3 : Security assurance requirements.
[CERTIF_SURV]	Procédure de surveillance des produits certifiés, version en vigueur Disponible sur http://www.ssi.gouv.fr
[SOGIS-CRYPTO]	SOG-IS Crypto Evaluation Scheme - Agreed Cryptographic Mechanisms - Version 1.0 – May 2016 Disponible sur http://sogis.org
[CC]	ISO/IEC 15408:2005 Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model; Part 2: Security functional requirements; Part 3: Security assurance requirements.
[CRITERES_OEC]	Organismes d'évaluation de la conformité – Critères de reconnaissance au titre du règlement eIDAS, version en vigueur. Disponible sur http://www.ssi.gouv.fr
[PSCO_QUALIF]	Prestataires de services de confiance qualifiés - Critères d'évaluation de la conformité au règlement eIDAS, version en vigueur Disponible sur http://www.ssi.gouv.fr

II. Annexe 2 - Engagements relatifs au suivi de sécurité du produit

Le commanditaire de la certification de conformité du DCSQ/DCCQ s'engage à :

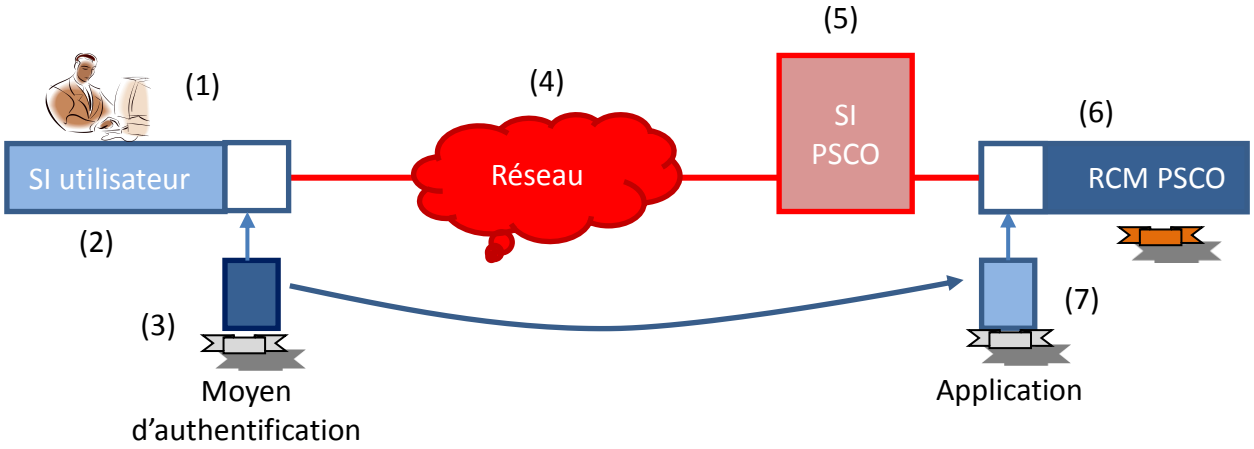
- Assurer une veille de la sécurité du dispositif certifié afin d'identifier au plus tôt tout vulnérabilité relative au dispositif certifié ;

- Informer sans délai et par écrit l'ANSSI et l'ensemble des utilisateurs du dispositif certifié de :
    - Toute publication de correctif de sécurité relatif au dispositif certifié ;
    - Tout arrêt de la veille sécurité relative au dispositif certifié ;

- Informer sans délai et par écrit l'ANSSI de la découverte de toute vulnérabilité affectant ou susceptible d'affecter le dispositif certifié. Pour chaque vulnérabilité, le commanditaire fournit :
    - La description de la vulnérabilité et de son niveau de gravité à partir de l'analyse de son impact, des conditions de son exploitation et de sa publicité ;
    - L'identifiant du correctif de sécurité permettant d'empêcher l'exploitation de la vulnérabilité lorsqu'il existe ou la date prévisionnelle de publication du correctif de sécurité le cas échéant ;
    - La description des mesures techniques ou organisationnelles palliatives temporaires, lorsqu'elles existent, permettant d'empêcher l'exploitation de la vulnérabilité ou d'en limiter les impacts dans l'attente de la publication d'un correctif de sécurité ;

- Informer sans délai et par écrit l'ANSSI de :
    - Tout incident de sécurité affectant ou susceptible d'affecter le dispositif certifié ;
    - Tout incident de sécurité affectant ou susceptible d'affecter un système d'information impliqué dans la spécification, la conception, le développement, la fabrication, l'exploitation, l'administration, la maintenance, l'avant-vente, le support technique ou la livraison du dispositif certifié ;
    - Tout incident de sécurité affectant ou susceptible d'affecter les données sensibles relatives aux utilisateurs du dispositif certifié, que ces données soient à caractère personnel ou non.

III. Annexe 3 - Exemple d'implémentation de DCSQ et DCCQ mis en œuvre par un PSCo qualifié



Typiquement, un service (5) accessible via un réseau qui n'est pas de confiance (4) permet de signer des données qui lui sont transmises par un signataire (1) via son système d'information (2). Les principales exigences de l'annexe II du règlement [eIDAS] sont rappelées ci-après avec un commentaire sur ce que cela implique :

- « la confidentialité des données de création de signature électronique utilisées pour créer la signature électronique est suffisamment assurée » et
- « les données de création de signature électronique utilisées pour créer la signature électronique ne peuvent être pratiquement établies qu'une seule fois » et
- « l'on peut avoir l'assurance suffisante que les données de création de signature électronique utilisées pour créer la signature électronique ne peuvent être trouvées par déduction et que la signature électronique est protégée de manière fiable contre toute falsification par les moyens techniques actuellement disponibles ».

En pratique, cela implique l'utilisation d'une RCM (6) et d'une cryptographie à l'état de l'art. Cela implique également une utilisation adaptée de la RCM dans laquelle le fournisseur de service ne doit pas avoir la capacité technique de mettre en œuvre la clé d'un utilisateur du service sans son consentement express.

- « les données de création de signature électronique utilisées pour créer la signature électronique peuvent être protégées de manière fiable par le signataire légitime contre leur utilisation par d'autres ».

Cela implique une authentification forte (3) entre le signataire et la RCM (6), cette authentification permettant le déclenchement du calcul de la signature, et permettant d'établir un canal sécurisé entre le moyen local par lequel l'utilisateur s'authentifie et la RCM distante.

Par analogie avec le cas précédent, **la RCM(6) doit être certifiée, dans le cadre de l'accord de reconnaissance européen SOG-IS, à un niveau de confiance comparable à celui demandé par les profils de protection référencés sur le site du SOG-IS (typiquement, EAL4+AVA_VAN.5…) mettant en œuvre un canal sécurisé entre le moyen local par lequel l'utilisateur s'authentifie et la RCM distante[7].**

[7] Par exemple, certifié selon le PP HSM CMCSO 14167-4 d'août 2015.

Note : En général, les certifications de RCM portent sur des fonctionnalités génériques et ne prennent pas en compte des enchaînements sécurisés d'opérations permettant de réaliser une fonctionnalité spécifique.

Dans le cas où cet enchainement d'opérations serait réalisé par le système d'information du prestataire de signature auquel est raccordée la RCM, tout ou partie du système d'information devrait être au même niveau de confiance que la RCM elle-même, avec les certifications correspondantes. La pratique montre que cet objectif est difficilement atteignable.

C'est pourquoi il est préconisé que l'enchaînement des opérations permettant de réaliser la signature électronique dans le cadre d'une session garantissant l'identité du signataire ainsi que l'intégrité des données transmises par le signataire soit assuré par une application (7) embarquée dans la RCM elle-même (6).

Si c'est le cas, l'application (7) réalisant ces fonctionnalités doit faire l'objet, au minimum, d'une certification CSPN, et il est recommandé qu'elle fasse l'objet d'une certification selon les critères communs au niveau EAL3+ dans le cadre de l'accord de reconnaissance européen SOG-IS. Par ailleurs, les spécifications cryptographiques garantissant l'authenticité du signataire et l'intégrité de la session doivent être fournies à l'ANSSI et doivent faire l'objet d'une évaluation de conformité par rapport au [SOGIS-CRYPTO] par un laboratoire agréé dans ce domaine.

Le système doit permettre d'assurer la confidentialité de la clé privée de l'utilisateur, à tout moment depuis sa génération jusqu'à sa destruction :

- Si la clé privée est générée dans la RCM, la preuve de possession de la clé privée, nécessaire à la requête de certificat, doit être générée sous le contrôle et avec le consentement de l'utilisateur ;
- Si la clé privée est générée dans un autre environnement (par exemple, par le PSCO délivrant le certificat de l'utilisateur), la RCM doit prévoir des mécanismes permettant de protéger son intégrité et sa confidentialité lors de son import, et les exigences de certification de la RCM s'appliquent sur le dispositif visant à générer cette clé privée.

L'aspect « à distance » introduit des risques supplémentaires par rapport à l'authentification locale. **L'authentification de l'utilisateur doit être forte (via l'emploi de deux facteurs distincts), et le dispositif d'authentification doit faire l'objet, au minimum, d'une certification CSPN**. Ce dispositif d'authentification doit être sous le contrôle exclusif de l'utilisateur, et mettre en œuvre des contrôles de sécurité de sorte qu'il soit hautement improbable que des activités telles que les tentatives de décryptage, l'écoute, l'attaque par rejeu ou la manipulation d'une communication par un attaquant ayant un potentiel d'attaque modéré puissent nuire aux mécanismes d'authentification. Le mécanisme d'authentification mis en œuvre doit être dynamique.

Par ailleurs, les spécifications cryptographiques doivent être fournies à l'ANSSI et doivent faire l'objet d'une évaluation de conformité par rapport au [SOGIS-CRYPTO] par un laboratoire agréé dans ce domaine.

Enfin, ce dispositif doit permettre d'assurer l'authenticité et protéger l'intégrité des données transmises par le signataire et concourant à la réalisation de la signature (données ou condensat des données à signer, référence à la clé de signature, etc.).