CERTIFICATION DE LA CONFORMITÉ AU RÉFÉRENTIEL GÉNÉRAL DE SÉCURITÉ DE LA PRINCIPAUTÉ DES DISPOSITIFS DE CRÉATION DE SIGNATURE ET DE CACHET ÉLECTRONIQUES QUALIFIÉS

Annexe à l'Arrêté Ministériel 2020-463
du 6 juillet 2020

ANNEXE AU « JOURNAL DE MONACO » N° 8.495

DU 17 JUILLET 2020

1. Introduction

1.1. Objet

La présente annexe décrit, dans le respect des règles posées par les articles 21, 22 et 30 de l'Arrêté Ministériel n° 2020-461 du 6 juillet 2020 portant application de l'article 13 de l'Ordonnance Souveraine n° 8.099 du 16 juin 2020 fixant les conditions d'application de la loi n° 1.383 du 2 août 2011 pour une Principauté numérique, modifiée, relative aux services de confiance, la procédure de délivrance, par l'Agence Monégasque de Sécurité Numérique, des certificats de conformité pour les Dispositifs de Création de Signature électronique Qualifiés (DCSQ), « Qualified electronic Signature Creation Device » (QSCD) en anglais, et Dispositifs de Création de Cachet électronique Qualifié (DCCQ), « Qualified electronic Seal Creation Device » (QSCD) en anglais.

L'Arrêté Ministériel n° 2020-461 du 6 juillet 2020, précité, prévoit que la création d'une signature électronique ou d'un cachet électronique dits « qualifiés », exige des dispositifs de création de signature électronique et de cachet électronique qui soient qualifiés. Les exigences applicables à ces dispositifs qualifiés sont définies dans l'Annexe III dudit arrêté.

Les conditions d'obtention d'un certificat de conformité pour un DCSQ / DCCQ sont précisées dans les paragraphes ci-après.

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

Les dispositifs de création de signature et/ou de cachet électroniques qualifiés certifiés conformément à la présente annexe sont présumés satisfaire aux exigences de l'Annexe III de l'Arrêté Ministériel n° 2020-461 du 6 juillet 2020, précité.

1.2. Mise à jour

La mise à jour de la présente annexe est réalisée par l'Agence Monégasque de Sécurité Numérique en fonction des évolutions législatives et règlementaires en matière de Sécurité des Systèmes d'Information. Ladite mise à jour est publiée par arrêté ministériel, lequel précise les modalités de transition et date d'effet.

1.3. Liste des abréviations

Les abréviations utilisées dans la présente annexe sont les suivantes :

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CC	Critères Communs / Common Criteria
CCRA	Arrangement de reconnaissance mutuelle selon les critères communs Common criteria recognition arrangement, voir : https://www.commoncriteriaportal.org
CSPN	Certification de Sécurité de Premier Niveau : https://www.ssi.gouv.fr/administration/produits-certifiés/cspn
DCCQ	Dispositif de création de cachet qualifié
DCSQ	Dispositif de création de signature qualifiée
HSM	Hardware Security Module. Enceinte sécurisée en mesure de protéger l'intégrité et la confidentialité de secrets et de réaliser des calculs cryptographiques en toute sécurité
PSCo	Prestataire de service de confiance
QSCD	Qualified electronic Signature Creation Device ou Qualified electronic Seal Creation Device, DCSQ ou DCCQ en français.
SSCD	Secure Signature Creation Device. Cf. règlement n° 910/2014 du Parlement européen et du Conseil 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 1999/93/CE eIDAS.
SOG-IS	Senior Officials Group-Information System Security. Accord européen pour la reconnaissance des certificats de sécurité (notamment CC). Voir https://www.sogis.org.
RGSP	Référentiel Général de Sécurité de la Principauté, prévu par l'arrêté ministériel n° 2020-461 du 6 juillet 2020 portant application de l'article 13 de l'Ordonnance Souveraine n° 8.099 du 16 juin 2020 fixant les conditions d'application de la loi n° 1.383 du 2 août 2011 pour une Principauté numérique, modifiée, relative aux services de confiance

2. Exigences relatives aux dispositifs de création de signature et cachet électroniques qualifiés

2.1. Processus d'attribution du certificat de conformité

2.1.1. Demande de certificat de conformité

La demande de certificat de conformité est adressée à l'Agence Monégasque de Sécurité Numérique. 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) délivré par l'organisme de certification de la conformité.

2.1.2. Forme du certificat de conformité de produit

Le certificat de conformité délivré par l'Agence Monégasque de Sécurité Numérique 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 (ou de cachet) pour le compte du signataire (ou 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.

2.1.3. Validité du certificat de conformité

Le certificat de conformité est lié au certificat de sécurité initial, typiquement le certificat reposant sur les [CC]. Or l'état de l'art des attaques, pour lesquels 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. Le processus de surveillance est défini par un texte émis par l'ANSSI sous la référence [CERTIF_SURV] et permet à cette dernière d'émettre un certificat de surveillance.

Ledit certificat de surveillance est attendu par l'Agence Monégasque de Sécurité Numérique dans un délai maximal de 5 ans après la décision de certification [CC] ou la dernière surveillance.

L'Agence Monégasque de Sécurité Numérique a 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 du processus de surveillance ou par tout autre fait porté à la connaissance de l'Agence Monégasque de Sécurité Numérique et qui remet en cause la conformité du dispositif aux exigences du Référentiel Général de Sécurité de la Principauté, l'Agence Monégasque de Sécurité Numérique 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 Appendice 4 de la présente annexe 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 2.3, selon le type de DCSQ ou DCCQ ayant fait l'objet de la certification de conformité.

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

Les dispositifs permettant la création d'une signature électronique qualifiée et d'un cachet électronique qualifié sont définis dans l'Arrêté Ministériel n° 2020-461 du 6 juillet 2020 portant application de l'article 13 de l'Ordonnance Souveraine n° 8.099 du 16 juin 2020 fixant les conditions d'application de la loi n° 1.383 du 2 août 2011 pour une Principauté numérique, modifiée, relative aux services de confiance, de la manière suivante :

« 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 III ;

« dispositif de création de cachet électronique », un dispositif logiciel ou matériel configuré servant à créer un cachet électronique ;

« dispositif de création de cachet électronique qualifié », un dispositif de création de cachet électronique qui satisfait aux exigences énoncées à l'Annexe III ;

L'évaluation de la conformité de ces dispositifs doit permettre de démontrer le respect des exigences applicables telles que précisées dans l'Annexe III « **Exigences applicables aux dispositifs de création de signature électronique qualifiés** » de l'Arrêté ministériel n° 2020-461 du 6 juillet 2020, précité :

1. Les dispositifs de création de signature électronique qualifiés garantissent au moins, par des moyens techniques et des procédures appropriées, 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 chiffre 1, 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 l'Annexe III de l'Arrêté Ministériel n° 2020-461 du 6 juillet 2020, précité, s'appliquent, en tant que de besoin, aux dispositifs de création de cachet électronique qualifiés.

La certification de la conformité à ces exigences est réalisée conformément aux normes énumérées à l'Appendice 3 de la présente annexe, relatives à l'évaluation de la sécurité des produits informatiques qui s'appliquent à la certification de DCSQ ou DCCQ.

Pour les DCSQ ou DCCQ pour lesquels les données de création de signature ou de cachet électroniques sont conservées dans un environnement sous le contrôle de l'utilisateur, la certification de conformité repose sur les normes référencées dans l'Appendice 1 de la présente annexe, dont les modalités d'application sont définies au paragraphe 2.3.1.

Pour les DCSQ ou DCCQ pour lesquels les données de création de signature ou de cachet électroniques 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 au paragraphe 2.3.2.

2.3. Modalités de certification de la conformité des DCSQ et DCCQ

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

a) Délivrance du certificat de conformité

Le certificat de conformité complet du DCSQ ou DCCQ est délivré si l'Agence Monégasque de Sécurité Numérique a pu vérifier 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 sur la base de l'un des profils de protection référencés dans l'appendice 3 ;

et

- la cryptographie répond aux règles définies dans le document « *SOG-IS Crypto Evaluation Scheme* ». 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'Agence Monégasque de Sécurité Numérique donne lieu à une inscription dans la liste des DCSQ/DCCQ certifiés prévue à l'article 23 de l'Arrêté Ministériel n° 2020-461 du 6 juillet 2020 portant application de l'article 13 de l'Ordonnance Souveraine n° 8.099 du 16 juin 2020 fixant les conditions d'application de la loi n° 1.383 du 2 août 2011 pour une Principauté numérique, modifiée, relative aux services de confiance.

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 sur le site de l'Agence Monégasque de Sécurité Numérique.

2.3.2. Lorsque les données de création de signature ou de cachet électroniques 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 si l'Agence Monégasque de Sécurité Numérique a pu vérifier 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 sur la base d'une cible de sécurité validée par l'Agence Monégasque de Sécurité Numérique[1] ;

1 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'appendice II du Règlement Général de Sécurité de la Principauté 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 l'appendice 3 de la présente annexe.

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'Agence Monégasque de Sécurité Numérique ;

et

- la cryptographie répond aux règles définies dans le document « *SOG-IS Crypto Evaluation Scheme* ». Cette vérification repose sur une analyse théorique des mécanismes cryptographiques et sur une expertise de leur implémentation.

L'appendice 2 de la présente annexe 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 l'Agence Monégasque de Sécurité Numérique pour inscription sur la liste des DCCQ/DCSQ certifiés prévue à l'article 23 de l'Arrêté Ministériel n° 2020-461 du 6 juillet 2020 portant application de l'article 13 de l'Ordonnance Souveraine n° 8.099 du 16 juin 2020 fixant les conditions d'application de la loi n° 1.383 du 2 août 2011 pour une Principauté numérique, modifiée, relative aux services de confiance. L'Agence Monégasque de Sécurité Numérique 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 l'Agence Monégasque de Sécurité Numérique a pu vérifier 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 ayant signé un accord conformément à l'article 4 de l'Arrêté Ministériel n° 2020-461 du 6 juillet 2020 portant application de l'article 13 de l'Ordonnance Souveraine n° 8.099 du 16 juin 2020 fixant les conditions d'application de la loi n° 1.383 du 2 août 2011 pour une Principauté numérique, modifiée, relative aux services de confiance ou dans la liste de confiance de la Principauté ;

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 III de l'Arrêté Ministériel n° 2020-461 du 6 juillet 2020, précité ;

et

- ce prestataire de services de confiance qualifié respecte les exigences du règlement applicable à l'ensemble des prestataires de services de confiance, précisées aux article 5 et 10 de l'Arrêté Ministériel n° 2020-461 du 6 juillet 2020, précité, 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 Référentiel Général de Sécurité de la Principauté applicables aux prestataires de services de confiance qualifiés, précisées dans l'Arrêté Ministériel n° 2020-461 du 6 juillet 2020 portant application de l'article 13 de l'Ordonnance Souveraine n° 8.099 du 16 juin 2020 fixant les conditions d'application de la loi n° 1.383 du 2 août 2011 pour une Principauté numérique, modifiée, relative aux services de confiance, sur l'environnement de mise en œuvre du DCSQ ou du DCCQ.

L'Agence Monégasque de Sécurité Numérique 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 publiée par l'ANSSI [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 mise en œuvre la clé privée de signature ou de cachet.

La délivrance d'un certificat de conformité complet par l'Agence Monégasque de Sécurité Numérique donne lieu à une inscription dans la liste des DCSQ/DCCQ certifiés prévue à l'article 23 de l'Arrêté Ministériel n° 2020-461 du 6 juillet 2020 portant application de l'article 13 de l'Ordonnance Souveraine n° 8.099 du 16 juin 2020 fixant les conditions d'application de la loi n° 1.383 du 2 août 2011 pour une Principauté numérique, modifiée, relative aux services de confiance. 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 mise 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'Agence Monégasque de Sécurité Numérique 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'Agence Monégasque de Sécurité Numérique ; et
- initie, dans un délai maximal de deux mois, tous travaux d'évaluation complémentaire demandés par l'Agence Monégasque de Sécurité Numérique.

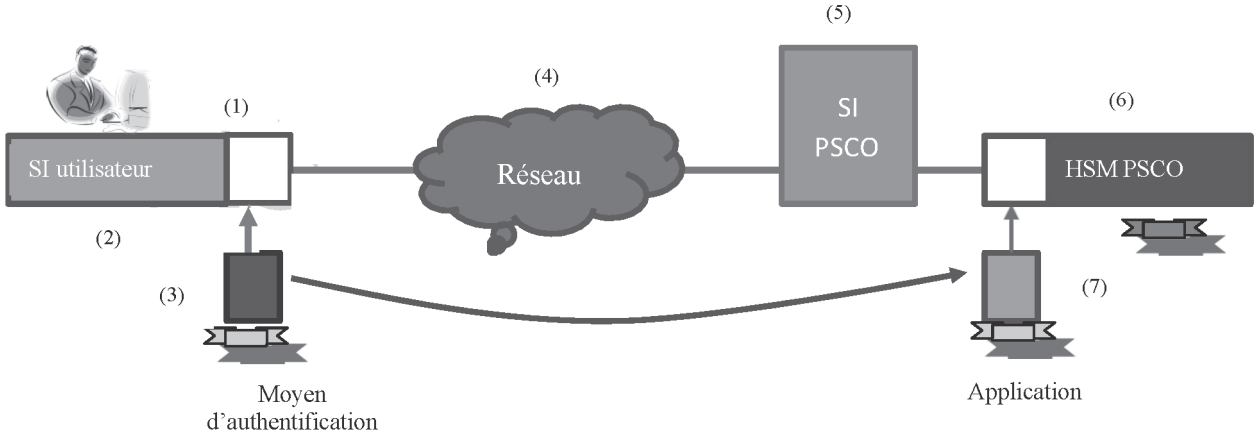
Une fois la décision de certification de conformité arrivée à échéance ou révoquée, le DCSQ/DCCQ est retiré de la liste publiée par l'Agence Monégasque de Sécurité Numérique.

APPENDICES

APPENDICE 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
[CC]	ISO/IEC 15408:2008-2009 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 l'ANSSI de surveillance des produits certifiés, version en vigueur disponible sur https://www.ssi.gouv.fr
[SOGIS-CRYPTO]	SOG-IS Crypto Evaluation Scheme - Agreed Cryptographic Mechanisms - Version 1.0 - May 2016 Disponible sur http://sogis.org
[CRITERES_OEC]	Organismes d'évaluation de la conformité - Critères de reconnaissance au titre du règlement eIDAS, version en vigueur. Disponible sur https://www.ssi.gouv.fr

APPENDICE 2 - EXEMPLES 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 Référentiel Général de Sécurité de la Principauté 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'un HSM (6) et d'une cryptographie à l'état de l'art. Cela implique également une utilisation adaptée du HSM 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 le HSM (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 le HSM distante.

Par analogie avec le cas précédent, le HSM (6) doit être certifié, 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 le HSM distant [1].

Note : En général, les certifications de HSM 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 raccordé le HSM, tout ou partie du système d'information devrait être au même niveau de confiance que le HSM lui-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 soit assuré par une application (7) embarquée dans le HSM lui-même (6).

---

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

Si tel 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'Agence Monégasque de Sécurité Numérique et doivent faire l'objet d'une évaluation de conformité par rapport au *SOG-IS Crypto Evaluation Scheme* 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 le HSM, 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), le HSM doit prévoir des mécanismes permettant de protéger son intégrité et sa confidentialité lors de son import, et les exigences de certification du HSM 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 (2 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'Agence Monégasque de Sécurité Numérique et doivent faire l'objet d'une évaluation de conformité par rapport au *SOG-IS Crypto Evaluation Scheme* 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.).

APPENDICE 3 - LISTE DES NORMES VISÉES À L'ARTICLE 2.2

• ISO/IEC 15408 - Technologies de l'information - Techniques de sécurité - Critères d'évaluation pour la sécurité TI - Parties 1 à 3, telles qu'elles sont énumérées ci-dessous :

- ISO/IEC 15408-1:2009 - Technologies de l'information - Techniques de sécurité - Critères d'évaluation pour la sécurité TI - Partie 1. ISO, 2009,
- ISO/IEC 15408-2:2008 - Technologies de l'information - Techniques de sécurité - Critères d'évaluation pour la sécurité TI - Partie 2. ISO, 2008,
- ISO/IEC 15408-3:2008 - Technologies de l'information - Techniques de sécurité - Critères d'évaluation pour la sécurité TI - Partie 3. ISO, 2008 ;

et

• ISO/IEC 18045:2008 - Technologies de l'information - Techniques de sécurité - Méthodologie pour l'évaluation de sécurité TI ;

et

• EN 419211 - Profils de protection pour dispositif sécurisé de création de signature électronique - Parties 1 à 6, selon le cas, telles qu'elles sont énumérées ci-dessous :

- EN 419211-1:2014 - Profils de protection pour dispositif sécurisé de création de signature électronique - Partie 1 : Présentation générale,
- EN 419211-2:2013 - Profils de protection des dispositifs sécurisés de création de signature - Partie 2 : Dispositif avec génération de clé,
- EN 419211-3:2013 - Profils de protection des dispositifs sécurisés de création de signature - Partie 3 : Dispositif avec import de clé,
- EN 419211-4:2013 - Profils de protection des dispositifs sécurisés de création de signature - Partie 4 : Extension pour un dispositif avec génération de clé et communication sécurisée avec l'application de génération de certificats,
- EN 419211-5:2013 - Profils de protection des dispositifs sécurisés de création de signature - Partie 5 : Extension pour un dispositif avec génération de clé et communication sécurisée avec l'application de création de signature,

- EN 419211-6:2014 - Profils de protection pour dispositif sécurisé de création de signature électronique - Partie 6 : Extension pour un dispositif avec import de clé et communication sécurisée avec l'application de création de signature.

APPENDICE 4 - 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 toute vulnérabilité relative au dispositif certifié ;
- Informer sans délai et par écrit l'Agence Monégasque de Sécurité Numérique 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'Agence Monégasque de Sécurité Numérique 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'Agence Monégasque de Sécurité Numérique 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.

imprimé sur papier recyclé

IMPRIMERIE GRAPHIC SERVICE
GS COMMUNICATION S.A.M. MONACO