Arrêté Ministériel n° 2018-69 du 30 janvier 2018 portant application de l'arrêté ministériel n° 2017‑835 du 29 novembre 2017 portant application l'article 54 de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée

Nous, Ministre d'État de la Principauté,

Vu la Constitution ;

Vu la loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives, modifiée ;

Vu la loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale ;

Vu l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée, et notamment son article 54 ;

Vu l'Ordonnance Souveraine n° 5.664 du 23 décembre 2015 créant l'Agence Monégasque de Sécurité Numérique, modifiée ;

Vu l'Ordonnance Souveraine n° 6.525 du 16 août 2017 portant application des articles 18, 19 et 25 de la loi n° 1.383 du 2 août 2011 sur l'économie numérique, modifiée ;

Vu l'arrêté ministériel n° 2016-723 du 12 décembre 2016, modifié, portant application de l'article 18 de la loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale et fixant les niveaux de classification des informations, modifié ;

Vu l'arrêté ministériel n° 2017-56 du 1er février 2017 portant application de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'administration et l'administré, modifiée ;

Vu l'arrêté ministériel n° 2017-835 du 29 novembre 2017 portant application de l'article 54 de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée ;

Vu l'arrêté ministériel n° 2018-66 du 30 janvier 2018 portant application de l'arrêté ministériel n° 2017-835 du 29 novembre 2017 portant application l'article 54 de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée ;

Vu la délibération du Conseil de Gouvernement en date du 17 janvier 2018 ;

ARRÊTONS :

ARTICLE PREMIER.

Les critères d'évaluation de la conformité au Référentiel Général de Sécurité, visé à l'annexe de l'arrêté ministériel n° 2017-835 du 29 novembre 2017, susvisé, des services de validation qualifiés des signatures électroniques qualifiées et des cachets électroniques qualifiés sont énoncés dans l'annexe au présent arrêté.

ART. 2.

Le Ministre d'État, le Conseiller de Gouvernement-Ministre des Affaires Sociales et de la Santé, le Conseiller de Gouvernement-Ministre de l'Équipement, de l'Environnement et de l'Urbanisme, le Conseiller de Gouvernement-Ministre de l'Intérieur, le Conseiller de Gouvernement-Ministre des Finances et de l'Économie et le Conseiller de Gouvernement-Ministre des Relations Extérieures et de la Coopération sont chargés, chacun en ce qui le concerne, de l'exécution du présent arrêté.

Fait à Monaco, en l'Hôtel du Gouvernement, le trente janvier deux mille dix-huit.

Le Ministre d'État,
S. TELLE.

CRITÈRES D'ÉVALUATION DE LA CONFORMITÉ AU RÉFÉRENTIEL GÉNÉRAL DE SÉCURITÉ DES SERVICES DE VALIDATION QUALIFIÉS DES SIGNATURES ÉLECTRONIQUES QUALIFIÉES ET DES CACHETS ÉLECTRONIQUES QUALIFIÉS

Annexe à l'arrêté ministériel n° 2018-69 du 30 janvier 2018

SOMMAIRE

1. Introduction

1.1. Objet

Conformément à l'Ordonnance Souveraine n° 5.664 du 23 décembre 2015, modifiée, susvisée, l'Agence Monégasque de Sécurité Numérique est l'autorité nationale en charge de la sécurité des systèmes d'information.

Elle est, en outre, l'organe de contrôle de la Principauté pour les prestataires de services de confiance et les services de confiance ayant notamment pour mission, de procéder à des contrôles aux fins de vérifier que lesdits prestataires et les services de confiance qualifiés qu'ils fournissent respectent les exigences du Référentiel Général de Sécurité, annexé à l'arrêté ministériel n° 2017-835 du 29 novembre 2017, susvisé, de vérifier l'existence des plans d'arrêt des services de confiance qualifiés et leur mise en œuvre effective ainsi que d'établir et tenir à jour la liste de confiance prévue au paragraphe 26 dudit référentiel.

La présente annexe décrit, dans le respect des règles posées par le Référentiel Général de Sécurité, précité, les exigences générales relatives aux critères d'évaluation de la conformité des services de validation qualifiés des signatures électroniques qualifiées et des cachets électroniques qualifiés. Ces exigences s'appliquent de manière cumulative avec celles décrites dans l'annexe à l'arrêté ministériel n° 2018-66 du 30 janvier 2018, susvisé, [PSCO_QUALIF] applicables à l'ensemble des prestataires de services de confiance qualifiés.

Seul le respect, par les services de validation qualifiés des signatures électroniques qualifiées et des cachets électroniques qualifiés mis en œuvre par un prestataire de services de confiance, des exigences générales déclinées au chapitre 2, permet de donner plein effet aux règles posées par le référentiel général de sécurité, précité, en ce qui concerne la validité des signatures électroniques qualifiées et des cachets électroniques qualifiés.

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 réglementaires 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 (de l'État français)
CSPN	Certification de Sécurité de Premier Niveau
OCSP	Online Certificate Status Protocol
PSCo	Prestataire de Services de Confiance

2. Exigences relatives aux services de validation des signatures et des cachets électroniques qualifiés

2.1. Modalités de qualification

2.1.1. Processus de qualification

Le processus de qualification d'un service de validation des signatures électroniques qualifiées et des cachets électroniques qualifiés s'inscrit dans le processus de qualification du prestataire de services de confiance tel que défini dans l'annexe à l'arrêté ministériel n° 2018-66 du 30 janvier 2018, précité [PSCO_QUALIF].

2.1.2. Inscription à la liste de confiance

Un service de validation qualifié des signatures et des cachets électroniques qualifiés est identifié dans la liste de confiance visée au paragraphe 26 du Référentiel Général de Sécurité, précité :

- au moyen du certificat électronique utilisé pour apposer le cachet du PSCo sur le rapport de validation ; ou
- au moyen du certificat électronique d'une autorité de certification opérée sous la responsabilité du PSCo qualifié, uniquement pour ses propres besoins, et ne délivrant pas de certificats pour des services de validation non qualifiés.

Dans le premier cas, si plusieurs certificats de cachet électronique sont mis en œuvre pour un même service de validation qualifié, cela donne lieu à l'inscription de plusieurs services dans la liste de confiance.

Dans le second cas, l'évaluation de la conformité doit permettre de démontrer que cette autorité de certification ne délivre des certificats qu'à l'attention exclusive de services de confiance opérés par le PSCo qualifié, et que celui-ci a mis en place des mesures organisationnelles et techniques appropriées afin d'assurer qu'aucun des certificats délivrés n'est utilisé par un service de validation non qualifié.

2.2. Critères d'évaluation de la conformité

L'évaluation doit permettre de démontrer le respect des exigences du Référentiel Général de Sécurité applicables aux services de validation des signatures électroniques qualifiées et des cachets électroniques qualifiés, spécifiées dans les paragraphes suivants dudit référentiel :

23 - 2. e)	Utilisation de systèmes et des produits fiables, sécurité et fiabilité des processus ;
23 - 2. h)	Conservation des données d'un service de validation des signatures électroniques et des cachets électroniques ;
23 - 2. i)	Plan d'arrêt d'activité d'un service de validation des signatures électroniques et des cachets électroniques ;
34 - 1.	Processus de validation d'une signature électronique qualifiée, permettant de vérifier que ;
34 - 1. a)	Le certificat sur lequel repose la signature était, au moment de la signature, un certificat qualifié de signature électronique conforme à l'annexe I ;
34 - 1. b)	Le certificat qualifié a été délivré par un prestataire de services de confiance qualifié et était valide au moment de la signature ;
34 - 1. c)	Les données de validation de la signature correspondent aux données

	communiquées à la partie utilisatrice ;
34 - 1. d)	L'ensemble unique de données représentant le signataire dans le certificat est correctement fourni à la partie utilisatrice ;
34 - 1. e)	L'utilisation d'un pseudonyme est clairement indiquée à la partie utilisatrice, si un pseudonyme a été utilisé au moment de la signature ;
34 - 1. f)	La signature électronique a été créée par un dispositif de création de signature électronique qualifié ;
34 - 1. g)	L'intégrité des données signées n'a pas été compromise ;
34 - 1. h)	Les exigences relatives à la signature électronique avancée (art. 26) ont été satisfaites au moment de la signature ;
35 - 1. a)	Respect des exigences faisant l'objet du paragraphe 34, chiffre 1 ;
35 - 1. b)	Fourniture aux parties utilisatrices du résultat du processus de validation, de manière automatisée, fiable, efficace et portant la signature électronique avancée ou le cachet électronique avancé du prestataire fournissant le service de validation qualifié ;
42	Application, en tant que de besoin, des paragraphes 34 et 35 à la validation des cachets électroniques qualifiés.

Le respect des exigences de la norme européenne ETSI [EN_319_401] relatives à la conservation des données et au plan d'arrêt d'activité, du processus de validation défini dans la norme européenne ETSI [EN_319_102] et des compléments précisés dans le chapitre 2.3, permet d'apporter une présomption de conformité à ces exigences.

2.3. Compléments aux différentes normes européennes ETSI [EN_319_401] et [EN_319_102]

2.3.1. Compléments relatifs à la fourniture du résultat de la validation d'une signature ou d'un cachet électronique qualifié

Le processus de validation doit permettre de fournir à la partie utilisatrice le résultat du processus de validation, de manière automatisée, fiable, efficace et portant la signature électronique avancée ou le cachet électronique avancé du prestataire fournissant le service de validation qualifié.

La norme européenne ETSI [EN_319_102] précise que le résultat du processus de validation est fourni via un rapport de validation permettant l'étude détaillée des décisions prises durant la phase de validation et la justification du statut de validation.

Le PSCo doit permettre l'accès au service de validation de signature ou de cachet, et la mise à disposition des parties utilisatrices de ce rapport de validation, de manière automatisée.

Afin de garantir la bonne interprétation du rapport de validation, le PSCo doit également rendre publique sa politique de validation des signatures électroniques qualifiées ou des cachets électroniques qualifiés.

2.3.2. Compléments relatifs à la signature ou au cachet du rapport de validation

Le processus de validation doit permettre de fournir à la partie utilisatrice le résultat du processus de validation, de manière automatisée, fiable, efficace et portant la signature électronique avancée ou le cachet électronique avancé du prestataire fournissant le service de validation qualifié.

Les modules cryptographiques employés pour apposer la signature électronique avancée ou le cachet électronique avancé du prestataire sur le rapport de validation de signature électronique qualifiée, ou de cachet électronique qualifié, doivent être conformes aux règles définies dans l'annexe à l'arrêté ministériel n° 2018-66 du 30 janvier 2018, précité [PSCO_QUALIF].

Il est recommandé que le certificat sur lequel repose cette signature électronique ou ce cachet électronique soit un certificat qualifié.

2.3.3. Compléments relatifs à la protection des applications de validation

Le prestataire de service de validation qualifié doit démontrer la mise en place de mesures techniques et organisationnelles permettant de réduire les risques pesant sur l'application utilisée pour la validation.

Il est recommandé que l'application de validation de signature ou de cachet ait fait l'objet d'une Certification de Sécurité de Premier Niveau (CSPN) selon une cible de sécurité vérifiée par l'ANSSI.

2.3.4. Compléments relatifs à la conservation des informations délivrées et reçues

Les exigences de la clause 7.10 de la norme européenne ETSI [EN_319_401] s'appliquent.

Le prestataire de service de validation qualifié doit conserver pendant une durée minimale de sept (7) ans après la date de validation de la signature électronique qualifiée ou du cachet électronique qualifié toutes les informations pertinentes concernant les données délivrées et reçues, notamment à fin de pouvoir fournir des preuves en justice. Le prestataire de service de validation qualifié précise dans ses conditions générales d'utilisation la durée de conservation effectivement appliquée ainsi que, le cas échéant, les modalités de réversibilité et de portabilité.

Toutes les informations pertinentes, transmises par le demandeur ou recueillies électroniquement pour la validation de la signature électronique ou du cachet électronique, doivent être conservées pendant sept (7) ans, dont au moins :

- la date et l'heure de la validation de la signature ou du cachet électronique qualifié ;
- les données fournies par le demandeur pour la validation de signature ou de cachet (valeur de la signature électronique ou du cachet électronique si celle-ci est séparable du document signé ou représentation unique du document signé dans le cas contraire) ainsi que l'identité du demandeur si celui-ci a fait l'objet d'une identification pour l'accès au service ;
- les données externes (listes de confiance, listes de certificats révoqués, réponses OCSP, …) utilisées pour valider la signature ou le cachet ;
- le rapport contenant le résultat de la validation de la signature ou du cachet électronique qualifié.

2.3.5. Compléments relatifs à la continuité de service et à l'arrêt d'activité du PSCo

Les exigences des clauses 7.11 et 7.12 de la norme européenne ETSI [EN_319_401] s'appliquent.

En cas de cessation d'activités, le PSCo doit détruire les clés privées utilisées pour signer les rapports de validation.

2.3.6. Compléments relatifs à la date et l'heure présumées de la création de la signature électronique et du cachet électronique qualifiés

Le processus de validation doit permettre d'attester que :

- le certificat sur lequel repose la signature ou le cachet, était, au moment de la signature ou de la création de cachet, un certificat de signature électronique qualifié ou un certificat de cachet électronique qualifié ;
- le certificat qualifié a été délivré par un prestataire de services de confiance qualifié et était valide au moment de la signature ou de la création de cachet.

Cette exigence impose la connaissance de la date et de l'heure de la création de la signature électronique qualifiée ou du cachet électronique qualifié afin de pouvoir vérifier au moment de la création de la signature électronique qualifiée ou du cachet électronique qualifié :

- que le certificat était bien dans sa période de validité ;
- que le certificat n'était pas révoqué ;
- que le prestataire de services ayant délivré le certificat était bien présent dans la liste de confiance, et que le service de délivrance de certificats correspondant avait bien le statut qualifié.

La date et l'heure de référence pour la validation sont la date et l'heure auxquelles la signature électronique ou le cachet électronique est fourni au service de validation dans les cas suivants :

- il n'y a pas de date et d'heure associées à la signature ou au cachet ; ou
- la date et l'heure se trouvent dans la signature ou le cachet sous la forme d'attributs renseignés par le signataire.

Si la date et l'heure sont associées à la signature ou au cachet au moyen d'un horodatage électronique non qualifié, il appartient au prestataire de service de validation qualifié d'accepter ou non comme référence de validation cette date et cette heure. En cas de non-acceptation, la date et l'heure de référence sont celles du moment de la validation. Le PSCo doit rendre publique sa politique d'acceptation des horodatages non qualifiés (incluant les modalités de vérification des jetons d'horodatage électronique).

Si la date et l'heure sont associées à la signature ou au cachet grâce à un horodatage électronique qualifié, cette date et cette heure sont prises comme référence pour la validation. Le PSCo doit mener l'ensemble des opérations techniques nécessaires à la validation du jeton d'horodatage, dont notamment :

- les vérifications relatives à la cryptographie (vérification de l'empreinte et de la signature figurant dans le jeton d'horodatage) ; et
- les vérifications des informations relatives à ce service d'horodatage électronique qualifié dans la liste de confiance, conformément aux prescriptions du standard ETSI [TS_119_612] (statut qualifié du service, présence du certificat de l'unité d'horodatage électronique ou de l'autorité de certification émettrice dans cette liste).

2.3.7. Compléments relatifs à la fraîcheur des informations de révocation

Le service de validation doit systématiquement solliciter les informations les plus récentes mises à disposition par l'autorité de certification émettrice du certificat qualifié. Si cette autorité met à disposition un service de répondeur OCSP, il est recommandé de s'appuyer sur celui-ci.

2.3.8. Compléments relatifs au statut qualifié du certificat de signature ou de cachet et du dispositif de création de signature ou de cachet

Le processus de validation doit permettre d'attester que :

- le certificat sur lequel repose la signature ou le cachet, était, au moment de la signature ou de la création de cachet, un certificat de signature électronique qualifié ou un certificat de cachet électronique qualifié ;
- la signature électronique ou le cachet électronique a été créé par un dispositif de création de signature / cachet électronique qualifié.

La présence des extensions de certificat suivantes, valorisées de la manière prévue par la norme européenne ETSI [EN_319_412-5], doit être vérifiée :

- « id-etsi-qcs-QcCompliance » ;
- « id-etsi-qcs-QcSSCD ».

La présence de l'extension « id-etsi-qcs-QcType » et sa bonne valorisation devraient être vérifiées, mais par mesure de compatibilité avec les certificats émis au titre de la directive 1999/93/EC du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques, abrogée, l'absence de cette extension ne devrait pas entrainer un rejet de la signature ou du cachet.

Dans le cas où cette extension est absente du certificat, la liste de confiance doit contenir une extension « additionalServiceInformation », valorisée de la manière prévue par le chapitre 5.5.9.4 du standard ETSI [TS_119_612] (« http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures »).

2.3.9. Compléments relatifs à la vérification du statut qualifié du prestataire de services de confiance ayant délivré le certificat de signature ou de cachet

Le processus de validation doit permettre d'attester que :

- le certificat sur lequel repose la signature ou le cachet, était, au moment de la signature ou de la création de cachet, un certificat de signature électronique qualifié ou un certificat de cachet électronique qualifié ;
- le certificat qualifié a été délivré par un prestataire de services de confiance qualifié et était valide au moment de la signature ou de la création de cachet.

La vérification de la liste de confiance permet de s'assurer que le certificat de signature ou de cachet électronique qualifié a été délivré par un prestataire de services de confiance qualifié, pour lequel :

- le champ « Service Type Identifier » est valorisé de la manière suivante « URI ; http://uri.etsi.org/TrstSvc/Svctype/CA/QC » ;
- le champ « Service Type Identifier » contient le certificat d'une Autorité de Certification à partir de laquelle un chemin de validation peut être construit jusqu'au certificat qualifié de signature ou de cachet.

Cette vérification doit :

- prendre comme référence la date et l'heure de début de validité figurant dans le certificat qualifié pour déterminer si, à la date présumée de délivrance du certificat, le prestataire de services de confiance ayant délivré le certificat était qualifié ;
- prendre comme référence la date et l'heure identifiées conformément aux règles du chapitre 2.3.6, pour déterminer si à, la date présumée de création de la signature ou du cachet, le prestataire de services de confiance ayant délivré le certificat était qualifié ;

- exploiter si nécessaire les informations sur les historiques des statuts des services de confiance qualifiés dans les listes de confiance, conformément aux clauses 5.5.9, 5.5.10 et 5.6 du standard ETSI [TS_119_612].

2.3.10. Compléments relatifs à l'identité du signataire ou du créateur de cachet

Le processus de validation permet d'attester que :

- l'ensemble unique de données représentant le signataire dans le certificat est correctement fourni à la partie utilisatrice ;
- l'utilisation d'un pseudonyme est clairement indiquée à la partie utilisatrice, si un pseudonyme a été utilisé au moment de la signature.

La présence du champ « Subject », valorisé de la manière prévue par les normes européennes ETSI [EN_319_412-2] et [EN_319_412-3], doit être vérifiée[1].

L'identité extraite du champ « Subject », et une mention relative à l'utilisation d'un pseudonyme le cas échéant, doit être précisée dans le rapport de validation.

[1] Ces normes représentent une bonne pratique mais ne sont pas d'application obligatoire. Le processus de validation doit pouvoir tolérer des écarts à celles-ci tant que l'exigence du 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 est remplie. À titre d'exemple, un certificat de signature électronique qualifié pourrait contenir un attribut commonName, mais pas d'attribut givenName ou surname.

Appendice : Références documentaires

Renvoi	Document
[RGS]	Référentiel Général de Sécurité, annexe à l'arrêté ministériel n° 2017-835 du 29 novembre 2017 portant application l'article 54 de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée
[EN_319_401]	ETSI EN 319 401 V2.1.1 (2016-02) : Electronic Signatures and Infrastructures (ESI) ; General Policy Requirements for Trust Service Providers
[EN_319_412-2]	ETSI EN 319 412-2 V2.1.1 (2016-02) : Part 2 : Certificate profile for certificates issued to natural persons
[EN_319_412-3]	ETSI EN 319 412-3 V1.1.1 (2016-02) : Part 2 : Certificate profile for certificates issued to legal persons
[EN_319_412-5]	ETSI EN 319 412-5 V2.1.1 (2016-02) : Part 5 : QCStatements
[EN_319_102]	Draft ETSI EN 319 102-1 V1.0.0 (2015-07) : Electronic Signatures and Infrastructures (ESI) ; Procedures for Creation and Validation of AdES Digital Signatures ; Part 1 : Creation and Validation
[TS_119_612]	ETSI TS 119 612 V2.1.1 (2015-07) : Electronic Signatures and Infrastructures (ESI) ; Trusted Lists
[PSCO_QUALIF]	Prestataires de services de confiance qualifiés - Critères d'évaluation de la conformité au RGS. Arrêté ministériel n° 2018-66 du 30 janvier 2018 Disponible sur https://amsn.gouv.mc
[1999/93/EC]	Directive du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques