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

Annexe à l'arrêté ministériel n° 2018-70
du 30 janvier 2018

ANNEXE AU « JOURNAL DE MONACO » N° 8.368

DU 9 FÉVRIER 2018

SOMMAIRE

1. Introduction 2

1.1. Objet 2

1.2. Mise à jour 2

1.3. Liste des abréviations.....3

2. Exigences relatives aux services de conservation qualifiés des signatures et des cachets électroniques qualifiés 3

2.1. Modalités de qualification 3

2.1.1. Processus de qualification 3

2.1.2. Inscription dans la liste de confiance ..3

2.2. Critères d'évaluation de la conformité.....3

2.3. Compléments aux différentes normes [EN_319_401], [TS_101_533-1], [ISO_14641-1] et [EN_319_102-1] 4

2.3.1. Compléments relatifs à l'utilisation de systèmes et produits fiables.....4

2.3.2. Compléments relatifs à la conservation des informations délivrées et reçues.....4

2.3.3. Compléments relatifs à la continuité de service et à l'arrêt d'activité du PSCo 4

2.3.4. Compléments relatifs aux procédures et technologies mises en œuvre pour étendre la fiabilité des signatures et cachets électroniques qualifiés.....5

Annexe - Références documentaires.....5

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 conservation qualifiés des signatures 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 conservation 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 fiabilité, au-delà de la période de validité technologique, 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 le présent document sont les suivants :

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
PSCo	Prestataire de Services de Confiance
WORM	Write Once Read Many

2. Exigences relatives aux services de conservation qualifiés 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 conservation qualifié des signatures 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 dans la liste de confiance

Un service de conservation 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 par le PSCo pour apposer un cachet ou un horodatage sur l'accusé de réception de la demande de conservation ; 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 conservation non qualifiés.

Dans le premier cas, si plusieurs certificats de cachet électronique sont mis en œuvre pour un même service de conservation 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 conservation non qualifié.

Le Référentiel Général de Sécurité n'impose pas qu'un accusé de réception soit transmis lors du dépôt d'une signature ou d'un cachet électronique qualifié auprès d'un service de conservation. Pour autant, il s'agit d'une bonne pratique aujourd'hui généralement appliquée par les prestataires de services d'archivage électronique.

Dans le cas où le PSCo n'émet pas d'accusé de réception faisant l'objet d'un cachet électronique, la demande de qualification devra préciser l'élément d'identification devant représenter le service dans la liste de confiance et justifier de sa pertinence au regard de la clause 5.5.3 du standard ETSI [TS_119_612].

2.2. Critères d'évaluation de la conformité

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

• 23(2).e Utilisation de systèmes et produits fiables pour la conservation des signatures électroniques et des cachets électroniques ;

• 23(2).h Conservation des données d'un service de conservation des signatures électroniques et des cachets électroniques ;

• 23(2).i Plan d'arrêt d'activité d'un service de conservation des signatures électroniques et des cachets électroniques ;

• 36(1) Utilisation de procédures et technologies permettant d'étendre la fiabilité des signatures électroniques qualifiées au-delà de la période de validité technologique ;

• 42 Application, en tant que de besoin, de l'article 36 à la conservation 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, des exigences applicables[1] des normes française [NF_Z42-013] ou européenne ETSI [EN_319_102-1] selon l'approche retenue par le PSCo, et des compléments précisés dans le chapitre 2.3, permet d'apporter une présomption de conformité à ces exigences.

[1] Le chapitre II.3.4 du présent document précise, selon la méthode de conservation retenue par le PSCo, les exigences applicables

Deux approches sont reconnues pour assurer la conservation des signatures et cachets électroniques qualifiés :

- Une approche systémique reposant sur la protection en intégrité d'un système d'archivage électronique dans lequel seront conservés les signatures et cachets électroniques qualifiés. Dans ce cas la norme française [NF_Z42-013] (équivalente à la norme internationale [ISO_14641-1]) est la norme de référence ; ou
- Une approche spécifique reposant sur la protection en intégrité, unitairement, de chaque signature ou cachet électronique qualifié faisant l'objet d'une conservation, par le biais d'une extension régulière de la signature ou du cachet ou d'une capture régulière des informations de validation.

Le présent document précise ainsi, en fonction de l'approche retenue, les exigences applicables.

2.3. Compléments aux différentes normes [EN_319_401], [TS_101_533-1], [ISO_14641-1] et [EN_319_102-1]

2.3.1. Compléments relatifs à l'utilisation de systèmes et produits fiables

Les modules cryptographiques employés pour les opérations nécessaires au service de conservation qualifié, notamment les opérations de création de signature électronique, de création de cachet électronique, ou d'horodatage, doivent respecter les règles spécifiées dans l'annexe à l'arrêté ministériel n° 2018-66 du 30 janvier 2018, précité [PSCO_QUALIF].

2.3.2. 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.

En outre, lorsque le service de conservation qualifié s'appuie sur une approche de type archivage électronique comme indiqué au chapitre II.3.4), les exigences de la clause 5.6 de la norme AFNOR [NF_Z42-013] sont applicables. D'autres méthodes peuvent être acceptées sous réserve qu'elles apportent un niveau d'assurance équivalent.

Le prestataire de service de conservation qualifié doit conserver pendant une durée au moins égale à la durée de conservation des signatures ou cachets électroniques qualifiés, 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 conservation qualifié précise dans ses conditions générales d'utilisation, le cas échéant, la durée supplémentaire de conservation des preuves (au-delà de la durée de conservation des signatures et cachets électroniques qualifiés) effectivement appliquée ainsi que les modalités de réversibilité et de portabilité.

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

Le PSCo doit prévoir des modalités de réversibilité permettant de garantir l'intégrité et l'exploitabilité de l'ensemble des éléments reversés, soit vers le demandeur initial, soit vers un autre prestataire de services de conservation qualifié avec l'accord express du demandeur initial.

Ces éléments doivent être lisibles et intelligibles par leur destinataire, et doivent être dans un format permettant leur bonne exploitation :

Si les éléments reversés sont dans un format non standard, le PSCo doit fournir les spécifications correspondantes et si nécessaire les outils permettant leur lecture ;

En complément, si ces éléments font l'objet d'une protection en intégrité au moyen d'horodatages ou de cachets électroniques, il doit être possible pour le destinataire de valider ces horodatages ou ces cachets, ce qui suppose le recours à des certificats électroniques pour lesquels le statut de révocation, la chaine de confiance et la politique de certification sont accessibles (par exemple, il peut s'agir du certificat électronique identifiant le service dans la liste de confiance).

La fiabilité des signatures et cachets électroniques qualifiés ne doit pas être affectée par cette réversibilité.

Le PSCo peut refuser la conservation de signatures ou cachets électroniques fournis dans des formats propriétaires, s'il estime qu'il ne lui est pas possible d'assurer leur lisibilité dans le temps.

2.3.4. Compléments relatifs aux procédures et technologies mises en œuvre pour étendre la fiabilité des signatures et cachets électroniques qualifiés

Le PSCo peut choisir d'assurer la conservation des signatures et cachets électroniques qualifiés :

- soit par un archivage électronique, permettant de garantir l'intégrité des signatures et cachets électroniques qualifiés archivés ;

- soit par, de manière régulière, une extension des signatures et cachets électroniques qualifiés permettant, sur le long terme, de valider ces signatures et cachets électroniques ou une capture des informations permettant, au-delà de la période de validité technologique, de valider ces signatures et cachets électroniques.

Le PSCo peut utiliser d'autres techniques, pourvu qu'il démontre que celles-ci répondent à un niveau de sécurité similaire aux deux précédentes.

Quelle que soit la méthode retenue, il est recommandé que le PSCo assure la conservation du document faisant l'objet de la signature ou du cachet électronique, dans les mêmes conditions de protection en intégrité, notamment pour pallier au risque d'affaiblissement de la fonction de calcul d'empreinte liant le document et la signature ou le cachet.

2.3.4.1 Compléments relatifs à l'archivage électronique

Si le PSCo met en œuvre un archivage électronique, les exigences de la norme AFNOR [NF Z42-013] s'appliquent. Le respect des exigences additionnelles définies dans la clause 4.2 de ladite norme n'est pas demandé.

Le PSCo doit également respecter les prescriptions du guide AFNOR [GA_Z42-019].

Lorsque le PSCo a recours à des supports réinscriptibles ou à des supports de type WORM logiques, les enregistrements doivent faire l'objet d'un horodatage électronique régulier, à une périodicité définie en fonction des résultats de l'analyse des risques et de l'état de l'art de la cryptographie. Il est recommandé que l'horodatage électronique soit qualifié.

Préalablement à son archivage, il est recommandé que la signature ou le cachet électronique qualifié fasse l'objet d'une validation par le prestataire de services de conservation qualifié, répondant aux exigences applicables aux services de validation qualifiés, telles que décrites dans l'annexe à l'arrêté ministériel n° 2018-69 du 30 janvier 2018 définissant les services de validation qualifiés des signatures électroniques qualifiées et des cachets électroniques qualifiés.

Le prestataire de services de conservation qualifié peut s'appuyer sur un prestataire de services de validation qualifié pour réaliser cette opération. Dans ce cas, la signature avancée ou le cachet électronique avancé, apposé par le prestataire de services de validation qualifié sur le rapport de validation, doit être vérifié avant l'archivage de la signature électronique qualifiée ou du cachet électronique qualifié.

Le résultat de la validation doit être archivé avec la signature ou le cachet électronique qualifié. Si le PSCo choisit de ne pas appliquer cette recommandation, il doit s'assurer que les utilisateurs du service sont bien informés de cette limitation et des risques induits par l'absence de validation initiale sur la fiabilité des signatures et cachets électroniques qualifiés conservés.

Le PSCo doit également pouvoir conserver, en complément des signatures et cachets électroniques qualifiés et dans les mêmes conditions de maintien d'intégrité, tous éléments additionnels transmis par le demandeur et concourant à prouver la validité de la signature ou du cachet électronique qualifié conservé.

Annexe - Références documentaires

Référence	Document
[EN_319_102-1]	Norme européenne ETSI EN 319 102-1 V1.1.1 (2016-05) Electronic Signatures and Infrastructures (ESI) Procedures for Creation and Validation of AdES Digital Signatures Part 1 : Creation and Validation
[EN_319_401]	Norme européenne ETSI EN 319 401 V2.1.1 (2016-02) : Electronic Signatures and Infrastructures (ESI) General Policy Requirements for Trust Service Providers
[GA_Z42-019]	Guide d'application de la norme AFNOR NF Z 42-013 (juin 2010)

[ISO_14641-1]	ISO 14641-1 (2012-02-01) : Electronic archiving Part 1 : Specifications concerning the design and the operation of an information system for electronic information preservation
[NF Z42-013]	Norme AFNOR NF Z42-013 (mars 2009) : Archivage électronique Spécifications relatives à la conception et à l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes
[PSCO_QUALIF]	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, relatif aux critères d'évaluation de la conformité au règlement général de sécurité des prestataires de services de confiance qualifiés
[TS_119_612]	Spécification ETSI TS 119 612 V2.1.1 (2015-07) : Electronic Signatures and Infrastructures (ESI) ; Trusted Lists

imprimé sur papier PEFC

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