CRITÈRES D'ÉVALUATION DE LA CONFORMITÉ AU RÉFÉRENTIEL GÉNÉRAL DE SÉCURITÉ DES SERVICES D'HORODATAGE ÉLECTRONIQUE QUALIFIÉS

Annexe à l'arrêté ministériel n° 2018-67
du 30 janvier 2018

ANNEXE AU « JOURNAL DE MONACO » N° 8.368

DU 9 FÉVRIER 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 relatives à la qualification de l'ensemble des services d'horodatage électronique.

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 d'horodatage électronique 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, des horodatages 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 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.

CSPN	Certification de Sécurité de Premier Niveau.
PH	Politique d'Horodatage.
PSHE	Prestataire de Services d'Horodatage Electronique.
RGS	Référentiel Général de Sécurité.

2. Exigences relatives aux services d'horodatage électronique qualifiés

2.1. Modalités de qualification

2.1.1. Processus de qualification

Le processus de qualification d'un service d'horodatage électronique s'inscrit dans le processus de qualification du prestataire de services de confiance, tel que décrit 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 d'horodatage qualifié est identifié dans la liste de confiance visée au paragraphe 26 du Référentiel Général de Sécurité, précité :

- au moyen du certificat électronique de l'unité d'horodatage ; ou
- au moyen du certificat électronique d'une autorité de certification opérée sous la responsabilité du PSHE qualifié, uniquement pour ses propres besoins, et ne délivrant pas de certificats pour des services d'horodatage électronique non qualifiés.

Dans le premier cas, si plusieurs unités d'horodatage sont mises en œuvre pour un même service d'horodatage électronique 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 PSHE 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 d'horodatage électronique 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, précité, applicables aux services d'horodatage électronique 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 d'horodatage électronique ;
23(2).i	Plan d'arrêt d'activité d'un service d'horodatage électronique ;
44(1).a	Lien entre date, heure, et données ;
44(1).b	Fondation sur une horloge exacte reliée à l'UTC ;
44(1).c	Signature ou cachet électronique avancé, ou méthode équivalente.

Le respect des exigences de la norme européenne ETSI [EN_319_421] et des compléments précisés dans le chapitre 2.3 du présent document, permet d'apporter une présomption de conformité à ces exigences.

2.3. Compléments à la norme européenne ETSI [EN_ 319_421]

2.3.1. Compléments relatifs à la certification des modules cryptographiques

Les modules cryptographiques employés pour générer les bi-clés de l'unité d'horodatage et pour signer les contremarques de temps doivent être conformes aux règles définies au chapitre 2.3.5 de l'annexe à l'arrêté ministériel n° 2018-66 du 30 janvier 2018, précité [PSCO_QUALIF].

2.3.2. Compléments relatifs à la protection des modules d'horodatage

Le lien entre la date et l'heure et les données est établi au moyen d'un module d'horodatage composé d'une application d'horodatage et d'un module cryptographique.

Si l'application d'horodatage est protégée dans l'environnement sécurisé du module cryptographique, alors l'application d'horodatage doit avoir fait l'objet au minimum d'une Certification de Sécurité de Premier Niveau (CSPN) selon une cible de sécurité vérifiée par l'ANSSI. Il est recommandé que l'application d'horodatage ait fait l'objet d'une certification selon les Critères Communs selon le profil de protection [CEN_419_231] ou [PP_HORODAT] édités sur le site web de l'ANSSI.

Si l'application d'horodatage n'est pas protégée dans l'environnement sécurisé du module cryptographique (par exemple, l'application d'horodatage fonctionne sur un serveur lui-même connecté au module cryptographique), alors le PSHE doit démontrer la mise en place de mesures techniques et organisationnelles permettant de réduire les risques pesant sur le module d'horodatage. Il est recommandé que l'application d'horodatage ait fait l'objet d'une Certification de Sécurité de Premier Niveau (CSPN) selon une cible de sécurité vérifiée par l'ANSSI.

2.3.3. Compléments relatifs à la conservation des données

Le PSHE doit conserver pendant une durée minimale de sept (7) ans après l'expiration de chaque jeton d'horodatage toutes les informations pertinentes concernant les données délivrées et reçues, notamment à fin de pouvoir fournir des preuves en justice. Le PSHE 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.

Appendice : Références documentaires

Renvoi	Document
[CEN_419_231]	Standard ETSI « Protection profile for trustworthy systems supporting time stamping, 2015-11-02 ». Disponible sur : http://www.etsi.org *Ce document est encore à l'état de projet*
[EN_319_421]	Norme européenne ETSI EN 319 421 v1.1.1 (2016-03), Electronic Signatures and Infrastructures (ESI) ; Policy and Security Requirements for Trust Service Providers issuing Time-Stamps. Disponible sur : http://www.etsi.org
[PP_HORODAT]	Profil de protection, Système d'horodatage, référence PP-SH-CCv3.1, version 1.7 du 18 juillet 2008, édité par l'ANSSI
[PSCO_QUALIF]	Arrêté ministériel n° 2018-66 du 30 janvier 2018 portant application de l'arrêté ministeriel 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 a 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
[PSHE_RGS]	Services d'horodatage électronique qualifiés - Modalités de qualification selon le RGS des services qualifiés selon le RGS
[RGS]	Référentiel Général de Sécurité, annexe à l'arrêté 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

imprimé sur papier PEFC

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