



Premier ministre

**Agence nationale de la sécurité
des systèmes d'information**

Services d'horodatage électronique qualifiés

Critères d'évaluation de la conformité au règlement eIDAS

Version 1.1 du 3 janvier 2017

HISTORIQUE DES VERSIONS			
DATE	VERSION	EVOLUTION DU DOCUMENT	REDACTEUR
04/05/2016	1.0	Version pour application au 1 ^{er} juillet 2016.	ANSSI
03/01/2017	1.1	Version pour application au 31 janvier 2017. <i>Modifications :</i> <ul style="list-style-type: none"> - <i>Précisions relatives à l'inscription dans la liste de confiance ;</i> - <i>Modifications mineures et clarifications.</i> 	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

Services d'horodatage électronique qualifiés – critères d'évaluation de la conformité au règlement eIDAS			
Version	Date	Critère de diffusion	Page
1.1	03/01/2017	PUBLIC	2/8

SOMMAIRE

I.	INTRODUCTION	4
I.1.	Objet.....	4
I.2.	Cadre juridique.....	4
I.3.	Mise à jour.....	4
I.4.	Acronymes	4
II.	EXIGENCES RELATIVES AUX SERVICES D'HORODATAGE ÉLECTRONIQUE QUALIFIÉS	5
II.1.	Processus de qualification	5
II.1.1.	<i>Modalités de qualification</i>	5
II.1.2.	<i>Considérations relatives à l'inscription dans la liste de confiance</i>	5
II.2.	Critères d'évaluation de la conformité.....	5
II.3.	Compléments à la norme [EN_ 319_421].....	6
II.3.1.	<i>Compléments relatifs à la certification des modules cryptographiques</i>	6
II.3.2.	<i>Compléments relatifs à la protection des modules d'horodatage</i>	6
II.3.3.	<i>Compléments relatifs à la conservation des données</i>	6
ANNEXES	7
I.	Annexe 1 Références documentaires.....	7
II.	Annexe 2 Couverture des exigences du règlement [eIDAS]	8

Services d'horodatage électronique qualifiés – critères d'évaluation de la conformité au règlement eIDAS			
Version	Date	Critère de diffusion	Page
1.1	03/01/2017	PUBLIC	3/8

I. Introduction

I.1. Objet

Dans le cadre du règlement [eIDAS], l'ANSSI, désignée comme organe de contrôle par la note des autorités françaises [NOTIFICATION], a la charge de contrôler le respect des exigences du règlement [eIDAS] par les prestataires de service de confiance qualifiés et les services de confiance qualifiés qu'ils fournissent.

La présente note décrit les exigences relatives à la qualification selon le règlement [eIDAS] des services d'horodatage électronique. Ces exigences s'appliquent de manière cumulative avec celles décrites dans la note [PSCO_QUALIF], applicables à l'ensemble des prestataires de services de confiance qualifiés.

Note : Si le service de confiance concerné est déjà qualifié selon le [RGS], il peut bénéficier des modalités de transition de la qualification selon le [RGS] vers la qualification selon le règlement [eIDAS], telles que définies dans la note [PSHE_RGS_eIDAS]. Dans ce cas, le présent document n'est pas applicable.

I.2. Cadre juridique

Les services d'horodatage électronique qualifiés, respectant les exigences spécifiées au chapitre II du présent document, bénéficient des effets juridiques définis à l'article 41 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.

I.4. Acronymes

Les acronymes utilisés dans le présent document sont les suivants :

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.

Services d'horodatage électronique qualifiés – critères d'évaluation de la conformité au règlement eIDAS			
Version	Date	Critère de diffusion	Page
1.1	03/01/2017	PUBLIC	4/8

II. Exigences relatives aux services d'horodatage électronique qualifiés

II.1. Processus de qualification

II.1.1. Modalités 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 la note [PSCO_QUALIF].

II.1.2. Considérations relatives à l'inscription dans la liste de confiance

Un service d'horodatage qualifié est identifié dans la liste de confiance :

- 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.

II.2. Critères d'évaluation de la conformité

L'évaluation doit permettre de démontrer le respect des exigences du règlement [eIDAS] applicables aux services d'horodatage électronique qualifiés, spécifiées dans les articles suivants :

- 24(2).e Utilisation de systèmes et des produits fiables, sécurité et fiabilité des processus ;
- 24(2).h Conservation des données d'un service d'horodatage électronique ;
- 24(2).i Plan d'arrêt d'activité d'un service d'horodatage électronique ;
- 42(1).a Lien entre date, heure, et données ;
- 42(1).b Fondation sur une horloge exacte reliée à l'UTC ;
- 42(1).c Signature ou cachet électronique avancé, ou méthode équivalente.

Le respect de la norme [EN_319_421] et des compléments précisés dans le chapitre II.3 du présent document permet d'apporter une présomption de conformité à ces exigences.

Services d'horodatage électronique qualifiés – critères d'évaluation de la conformité au règlement eIDAS			
Version	Date	Critère de diffusion	Page
1.1	03/01/2017	PUBLIC	5/8

II.3. Compléments à la norme [EN_ 319_421]

II.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 II.3.5 de la note [PSCO_QUALIF].

II.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].

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.

II.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 afin 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.

Services d'horodatage électroniques qualifiés – critères d'évaluation de la conformité au règlement eIDAS			
Version	Date	Critère de diffusion	Page
1.1	03/01/2017	PUBLIC	6/8

Annexes

I. Annexe 1 Références documentaires

Renvoi	Document
[CEN_419_231]	Protection profile for trustworthy systems supporting time stamping, 2015-11-02. Disponible sur : http://www.etsi.org <i>Ce document est encore à l'état de projet.</i>
[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
[EN_319_421]	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
[NOTIFICATION]	Note des autorités française du 17 février 2015 à la Commission, désignant l'ANSSI comme organe de contrôle au titre du règlement eIDAS.
[PP_HORODAT]	Profil de protection, Système d'horodatage, référence PP-SH-CCv3.1, version 1.7 du 18 juillet 2008. 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
[PSHE_RGS_EIDAS]	Services d'horodatage électronique qualifiés – Modalités de qualification selon le règlement eIDAS des services qualifiés selon le RGS, version en vigueur. Disponible sur http://www.ssi.gouv.fr
[RGS]	Référentiel général de sécurité, version 1 ou 2. Disponible sur http://www.ssi.gouv.fr

Services d'horodatage électronique qualifiés – critères d'évaluation de la conformité au règlement eIDAS			
Version	Date	Critère de diffusion	Page
1.1	03/01/2017	PUBLIC	7/8

II. Annexe 2 Couverture des exigences du règlement [eIDAS]

Article	Exigence du règlement eIDAS	Clauses applicables des normes européennes	Chapitres applicables du présent document
24(2).e	Utilisation des systèmes et des produits fiables	[EN_319_421] Clauses 7.6.2 et 7.6.3	Chapitres II.3.1 et II.3.2
24(2).h	Conservation des informations délivrées et reçues par le prestataire de services de confiance ;	[EN_319_421] Clause 7.12	Chapitre II.3.3
24(2).i	Continuité de service suite à l'arrêt d'activité du prestataire de services de confiance ;	[EN_319_421] Clause 7.14	<i>Pas de complément à la norme</i>
42(1).a	Lien entre date, heure, et données ;	[EN_319_421] Clauses 7.6.3 et 7.7.1	Chapitre II.3.2
42(1).b	Fondation sur une horloge exacte reliée à l'UTC	[EN_319_421] Clauses 7.7.1 et 7.7.2	<i>Pas de complément à la norme</i>
42(1).c	Signature ou cachet électronique avancé, ou méthode équivalente	[EN_319_421] Clause 7.7.1	Chapitre II.3.1

Services d'horodatage électronique qualifiés – critères d'évaluation de la conformité au règlement eIDAS			
Version	Date	Critère de diffusion	Page
1.1	03/01/2017	PUBLIC	8/8