Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Premier ministre

Agence nationale de la sécurité des systèmes d'information

Services de conservation qualifiés des signatures et des cachets électroniques qualifiés

Critères d'évaluation de la conformité au règlement eIDAS

Version 1.0 du 3 janvier 2017

HISTORIQUE DES VERSIONS			
DATE	**VERSION**	**EVOLUTION DU DOCUMENT**	**REDACTEUR**
23/06/2016	0.4	*Version de travail pour commentaires.*	ANSSI
03/01/2017	1.0	Version pour application au 31 janvier 2017. *Modifications :* - *Précisions relatives à l'inscription dans la liste de confiance ;* - *Ajouts de précisions relatives aux deux approches possibles, dans les critères d'évaluation de la conformité ;* - *Référence la norme française NF Z42-013 en remplacement dela norme ISO 14641-1 ;* - *Compléments relatifs à la réversibilité des éléments conservés en cas d'arrêt d'activité ;* - *Précisions relatives aux procédures et technologies mises en œuvre par le PSCo, selon l'approche retenue ;* - *Modifications mineures et clarifications.*	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

SOMMAIRE

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 par les prestataires de service de confiance qualifiés et la conformité des services de confiance qualifiés qu'ils fournissent.

La présente note décrit les critères d'évaluation de la conformité aux exigences du règlement [eIDAS] des services de conservation qualifiés des signatures et des cachets électroniques qualifiés. 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.

I.2. Cadre juridique

Les services de conservation qualifiés des signatures électroniques qualifiées et des cachets électroniques qualifiés mis en œuvre par un prestataire de services de confiance respectant les exigences spécifiées au chapitre II du présent document permettent d'apporter une présomption concernant la fiabilité, au-delà de la période de validité technologique, des signatures électroniques qualifiées et des cachets électroniques qualifiés tels que définis par le 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.
PSCo	Prestataire de Services de Confiance.
WORM	*Write Once Read Many.*

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

II.1. Modalités de qualification

II.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 décrit dans la note [PSCO_QUALIF].

II.1.2. Considérations relatives à l'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 :

- 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.

Note : Le règlement 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 [TS_119_612].

II.2. Critères d'évaluation de la conformité

L'évaluation doit permettre de démontrer le respect des exigences applicables du règlement [eIDAS] aux services de conservation qualifiés des signatures et des cachets électroniques qualifiés, spécifiées dans les articles suivants :

- 24(2).e Utilisation de systèmes et produits fiables, sécurité et fiabilité des processus ;
- 24(2).h Conservation des données d'un service de conservation des signatures électroniques et des cachets électroniques ;
- 24(2).i Plan d'arrêt d'activité d'un service de conservation des signatures électroniques et des cachets électroniques ;
- 34(1) Utilisation de procédures et technologies permettant d'étendre la fiabilité des signatures électroniques qualifiées au-delà de la période de validité technologique ;
- *40 Application mutatis mutandis de l'article 34 à la conservation des cachets électroniques qualifié.*

Le respect des exigences de la norme [EN_319_401] relatives à la conservation des preuves et au plan d'arrêt d'activité, des exigences applicables[1] des normes [NF_Z42-013] ou [EN_319_102-1] selon l'approche retenue par le PSCo, et des compléments précisés dans le chapitre II.3 du présent document, permet d'apporter une présomption de conformité à ces exigences.

Note : 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.

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

II.3. Compléments aux normes [EN_319_401], [NF_Z42-013] et [EN_319_102-1]

II.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 le cas échéant, doivent respecter les règles spécifiées dans le document [PSCO_QUALIF].

II.3.2. Compléments relatifs à la conservation des informations délivrées et reçues

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

Lorsque le service de conservation qualifié s'appuie sur une approche de type archivage électronique (voir le chapitre II.3.4 du présent document), les exigences de la clause 5.6 de la norme [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.

II.3.3. Compléments relatifs à la continuité de service et à l'arrêt d'activité du PSCo

Les exigences de la clause 7.12 de la norme [EN 319 401] s'appliquent.

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 et 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'agit 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.

Note : 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.

II.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 via le recours à un archivage électronique, permettant de garantir l'intégrité des signatures et cachets électroniques qualifiés archivés ;
- soit via le recours, de manière régulière, à une extension des signatures et cachets électroniques qualifiés ou à 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.

II.3.4.1. Compléments relatifs à l'archivage des signatures et cachets électroniques qualifiés

Si le PSCo met en œuvre un archivage électronique, les exigences de la norme [NFZ_42-013] s'appliquent. Le respect des exigences additionnelles définies dans la clause 4.2 de cette norme n'est pas demandé.

Le PSCo doit également respecter les prescriptions du guide [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 cet 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, tels que décrites dans la note [eIDAS_VAL_SIGN].

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.

Note : Le PSCo peut ne pas appliquer cette recommandation. Il doit dans ce cas s'assurer que les utilisateurs du service sont bien informés de cette limitation et des risques induits par l'absence de validation intiale 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.

II.3.4.2. Compléments relatifs à l'extension ou la capture des informations de validation des signatures et cachets électroniques qualifiés

Si le PSCo met en œuvre une extension régulière des signatures et cachets électroniques qualifiés, le processus décrit dans la clause 4.3.5 de la norme [EN_319_102-1] doit être appliqué.

La validation de la signature ou du cachet électronique qualifié doit répondre aux exigences applicables aux services de validation qualifiés, tels que décrites dans la note [eIDAS_VAL_SIGN].

Il est recommandé que le format des signatures et cachets électroniques qualifiés ayant fait l'objet de cette extension soit l'un de ceux prévus par les standards référencées dans la décision d'exécution [DEC_EXEC_1506].

Le PSCo peut, comme alternative à l'extension des signatures ou cachets électroniques qualifiés conservés, capturer régulièrement les informations nécessaires à leur validation (liste de confiance, informations relatives au statut de révocation). Il doit dans ce cas garantir l'intégrité et l'exploitabilité de ces éléments avec un niveau d'assurance au moins égal à celui permis par le mécanisme d'extension.

Annexes

I. Annexe 1 Références documentaires

	Document
[DEC_EXEC_1506]	Décision d'exécution (UE) 2015/1506 de la Commission du 8 septembre 2015 établissant les spécifications relatives aux formats des signatures électroniques avancées et des cachets électroniques avancés devant être reconnus par les organismes du secteur public visés à l'article 27, paragraphe 5, et à l'article 37, paragraphe 5, du règlement [eIDAS].
[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
[eIDAS_VAL_SIGN]	Services de validation qualifiés des signatures électronique qualifiées et des cachets électroniques qualifiés - Critères d'évaluation de la conformité au règlement eIDAS, version en vigueur. Disponible sur http://www.ssi.gouv.fr
[EN_319_102-1]	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]	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 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]	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.
[NOTIFICATION]	Note des autorités française du 17 février 2015 à la Commission, désignant l'ANSSI comme organe de contrôle au titre du règlement eIDAS.
[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
[TS_119_612]	ETSI TS 119 612 V2.1.1 (2015-07) : Electronic Signatures and Infrastructures (ESI); Trusted Lists.

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

Article	Exigence du règlement eIDAS	Clauses applicables des normes EN et ISO	Chapitres applicables du présent document
24(2).e	Utilisation de systèmes et produits fiables	[EN_319_401] Clause 7.7	II.3.1
24(2).h	Conservation des informations délivrées et reçues par le prestataire de services de confiance	[EN_319_401] Clause 7.10 [NF_Z42_013] V.6et [GA_Z42-019] (*archivage électronique*)	II.3.2
24(2).i	Continuité de service suite à l'arrêt d'activité du prestataire de services de confiance ;	[EN_319_401] Clause 7.12	II.3.3
34(1)	Utilisation de procédures et technologies permettant d'étendre la fiabilité des signatures électroniques qualifiées	[NF_Z42-013] et [GA_Z42-019] [EN_319_102-1] Clause 4.3.5 (*extension des signatures et cachets électroniques / capture des informations de validation*)	II.3.4
40	*Application mutatis mutandis de l'article 34 à la conservation des cachets électroniques qualifiés*		