Premier ministre

Agence nationale de la sécurité des systèmes d'information

Services de validation qualifiés des signatures électroniques qualifiées 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**
16/06/2016	0.8	*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 ;* - *Amendements aux exigences relatives à la conservation des données ;* - *Compléments relatifs à la vérification des jetons d'horodatage ;* - *Modification des exigences relatives à la fraicheur des informations de révocation ;* - *Précisions relatives à la vérification du statut qualifié du certificat de signature ou du cachet et à la récupération de l'identité du signataire ou créateur de cachet ;* - *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 validation qualifiés des signatures électroniques qualifiées 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 validation 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 sécurité juridique concernant la validité 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.
CSPN	Certification de Sécurité de Premier Niveau.
OCSP	*Online Certificate Status Protocol*.
PSCo	Prestataire de Services de Confiance.

II. Exigences relatives aux services de validation 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 validation 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 validation qualifié des signatures et des cachets électroniques qualifiés est identifié dans la liste de confiance :

- 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.

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 validation des signatures électroniques qualifiées 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 validation des signatures électroniques et des cachets électroniques ;
- 24(2).i Plan d'arrêt d'activité d'un service de validation des signatures électroniques et des cachets électroniques ;
- 32(1) Processus de validation d'une signature électronique qualifiée, permettant de vérifier que :
    - 32(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 ;
    - 32(1).b Le certificat qualifié a été délivré par un prestataire de services de confiance qualifié et était valide au moment de la signature ;
    - 32(1).c : Les données de validation de la signature correspondent aux données communiquées à la partie utilisatrice ;
    - 32(1).d : L'ensemble unique de données représentant le signataire dans le certificat est correctement fourni à la partie utilisatrice ;
    - 32(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 ;
    - 32(1).f : La signature électronique a été créée par un dispositif de création de signature électronique qualifié ;
    - 32(1).g : L'intégrité des données signées n'a pas été compromise ;
    - 32(1).h : Les exigences relatives à la signature électronique avancée (art.26) ont été satisfaites au moment de la signature ;
- 33(1).a Respect des exigences faisant l'objet de l'article 32, paragraphe 1 ;
- 33(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 ;
- *40 Application mutatis mutandis des articles 32 et 33 à la validation des cachets électroniques qualifiés.*

Le respect des exigences de la norme [EN_319_401] relatives à la conservation des données et au plan d'arrêt d'activité, du processus de validation défini dans la norme [EN_319_102] et des compléments précisés dans le chapitre II.3 du présent document, permet d'apporter une présomption de conformité à ces exigences.

II.3. Compléments aux normes [EN_319_401] et [EN_319_102]

II.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 [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.

Exigence : 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.

II.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.

Exigence : 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 la note [PSCO_QUALIF] ;

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

II.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.

Exigence : 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.

II.3.4. 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.

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 les modalités de réversibilité et de portabilité.

Exigence : 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.

II.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 [EN 319 401] s'appliquent.

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

II.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 :

- 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 ;

au moment de la création de la signature électronique qualifiée ou du cachet électronique qualifié.

Exigence : 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 [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).

II.3.7. Compléments relatifs à la fraicheur 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.

II.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.

Exigence : La présence des extensions de certificat suivantes, valorisées de la manière prévue par la norme [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, 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 [TS_119_612] (« *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures* »).

II.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 Digital Identity* » 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.

Exigence : 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 II.3.6 du présent document, 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 [TS_119_612].

II.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.

Exigence : La présence du champ « Subject », valorisé de la manière prévue par les normes [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 [eIDAS] est remplie. *A titre d'exemple, un certificat de signature électronique qualifié pourrait contenir un attribut commonName, mais pas d'attribut givenName ou surname.*

Annexes

I. Annexe 1 Références documentaires

Renvoi	Document
[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 319 401]	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.
[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 européennes	Chapitres applicables du présent document
24(2).e	Utilisation des systèmes et des produits fiables	[EN_319_401] Clause 7.7	Chapitres II.3.2 et II.3.3
24(2).h	Conservation des informations délivrées et reçues par le prestataire de services de confiance	[EN_319_401] Clause 7.0	Chapitre II.3.3
24(2).i	Continuité de service suite à l'arrêt d'activité du prestataire de services de confiance	[EN_319_401] Clause 7.12	*Pas de complément à la norme*
32(1).a	Qualification du certificat au moment de la signature	[EN_319_102] Clauses 5.2.6, 5.6.2	Chapitres II.3.6 et II.3.8
32(1).b	Délivrance du certificat par un PSCo qualifié et validité au moment de la signature	[EN_319_102] Clauses 5.2.5, 5.2.6, 5.6.2	Chapitres II.3.6, II.3.7 et II.3.9
32(1).c	Correspondance des données de validation de la signature aux données communiquées à la partie utilisatrice	[EN_319_102] Clause 5.2.7	*Pas de complément à la norme*
32(1).d	Fourniture correcte à la partie utilisatrice de l'ensemble unique de données représentant le signataire dans le certificat	[EN_319_102] Clause 5.2.3	Chapitre II.3.10
32(1).e	Indication claire à la partie utilisatrice de l'utilisation d'un pseudonyme, le cas échéant	*Non couvert*	Chapitre II.3.10
32(1).f	Création de la signature électronique par un dispositif de création de signature électronique qualifié	*Non couvert*	Chapitre II.3.8
32(1).g	Non compromission de l'intégrité des données signées	[EN_319_102] Clause 5.2.7	*Pas de complément à la norme*
32(1).h	Respect des exigences relatives à la signature électronique avancée	*Non couvert*	*Considéré comme couvert par les autres points de contrôle*
33(1).b	Fourniture aux parties utilisatrices du résultat du processus de validation, signé ou cacheté électroniquement par le prestataire	*Non couvert*	Chapitres II.3.1 et II.3.2
40	*Application mutatis mutandis des articles 32 et 33 à la validation des cachets électroniques qualifiés*		