Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Premier ministre

Agence nationale de la sécurité des systèmes d'information

Services de délivrance de certificats qualifiés de signature électronique, de cachet électronique et d'authentification de site internet

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**
20/06/2016	1.0	Version pour application au 1er juillet 2016.	ANSSI
03/01/2017	1.1	Version pour application au 31 janvier 2017. *Modifications :* - *Précisions relatives à l'inscription dans la liste de confiance ;* - *Précisions relatives à la vérification de l'identité du demandeur de certificat ;* - *Amendement des recommandations relatives à la fourniture du statut de révocation des certificats au-delà de leur période de validité, en accord avec l'évolution des normes ;* - *Précisions et corrections relatives aux profils de certificats recommandés ;* - *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 délivrance de certificats qualifiés de signature électronique, de cachet électronique et d'authentification de site internet. 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] au niveau deux étoiles (**) ou trois étoiles (***), 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 [PSCE_RGS_eIDAS]. Dans ce cas, le présent document n'est pas applicable.

I.2. Cadre juridique

Les certificats qualifiés de signature électronique, de cachet électronique et d'authentification de site internet délivrés par un prestataire de services de confiance respectant les exigences spécifiées au chapitre II du présent document sont présumés satisfaire aux exigences, respectivement, de l'annexe I, de l'annexe III et de l'annexe IV du règlement [eIDAS].

Les signatures électroniques avancées, reposant sur un certificat qualifié, et créées à l'aide d'un dispositif de création de signature électronique qualifié, sont des signatures électroniques qualifiées, bénéficiant des effets juridiques prévus à l'article 25 du règlement [eIDAS].

Les cachets électroniques avancés, reposant sur un certificat qualifié, et créés à l'aide d'un dispositif de création de cachet électronique qualifié, sont des cachets électroniques qualifiés, bénéficiant des effets juridiques prévus à l'article 35 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.
PSCE	Prestataire de Services de Certification Electronique.
RGS	Référentiel Général de Sécurité.
QSCD	*Qualified electronic Signature / Seal Creation Device*.
LCR	Liste des Certificats Révoqués.
OCSP	*Online Certificate Status Protocol.*
OID	*Object IDentifier*.
URL	*Uniform Resource Locator*.
http	*hypertext transfer protocol*.
LDAP	*Lightweight Directory Access Protocol*.

II. Exigences relatives aux services de délivrance de certificats qualifiés

II.1. Modalités de qualification

II.1.1. Processus de qualification

Le processus de qualification d'un service de délivrance de certificats qualifiés de signature électronique, de cachet électronique et d'authentification de site internet 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 délivrance de certificats qualifiés est identifié dans la liste de confiance au moyen du certificat électronique d'une autorité de certification racine, intermédiaire ou terminale.

L'évaluation de la conformité doit permettre de démontrer que, sous cette autorité de certification, il est possible de distinguer sans ambiguïté les certificats qualifiés et non qualifiés délivrés par celle-ci. En particulier, il est nécessaire de s'assurer que les certificats non qualifiés ne comportent pas d'attributs pouvant les faire considérer de manière erronée comme des certificats qualifiés.

Il est possible d'assortir cette identification de contraintes supplémentaires permettant d'identifier les certificats qualifiés délivrés sous cette autorité (*par exemple, au moyen d'un OID de politique de certification).*

Dans ce cas, l'évaluation de la conformité devra couvrir un périmètre cohérent avec les contraintes supplémentaires positionnées dans la liste de confiance (*par exemple, cette évaluation devra couvrir l'ensemble du périmètre relatif à un OID de politique de certification donné, et vérifier que cet OID n'est pas renseigné dans des certificats non qualifiés).*

Note : Afin de réduire le périmètre audité, il est recommandé d'identifier le service au moyen d'une autorité de certification terminale, délivrant uniquement des certificats qualifiés.

II.2. Critères d'évaluation de la conformité

L'évaluation doit permettre de démontrer le respect des exigences du règlement [eIDAS] applicables aux services de délivrance de certificats qualifiés de signature électronique, de cachet électronique et d'authentification de site internet, spécifiées dans les articles suivants :

- Pour les prestataires de services de confiance qualifiés délivrant des certificats qualifiés :
    - 24(1) Vérification de l'identité et des attributs spécifiques de la personne physique ou morale ;
    - 24(2).e Utilisation de systèmes et des produits fiables, sécurité et fiabilité des processus ;
    - 24(2).h Conservation des informations délivrées et reçues dans le cadre de la délivrance des certificats qualifiés ;
    - 24(2).i Continuité de service suite à l'arrêt d'activité de délivrance de certificats qualifiés ;
    - 24(2).k Base de données relative aux certificats émis ;
    - 24(3) Révocation des certificats ;
    - 24(4) Accès fiable, gratuit et efficace au statut de révocation des certificats.
- Pour les certificats qualifiés :
    - 28(1) Profils des certificats qualifiés de signature électronique ;
    - 28(3) Autorisation d'attributs spécifiques complémentaires non obligatoires ;
    - 28(4) Aspect relatifs à la révocation de ces certificats ;
    - 28(5) Aspects relatifs à la suspension de ces certificats ;
    - 38(1), (3), (4), (5) Profils des certificats qualifiés de cachet électronique, aspects relatifs à la révocation et suspension de ces certificats ;
    - 45(1) Profils des certificats qualifiés d'authentification de site Internet.

Le respect de la norme [EN 319 411-2] 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 à la norme [EN_319_411-2]

II.3.1. Compléments relatifs à la vérification de l'identité du demandeur

La vérification de l'identité de la personne physique ou morale à laquelle le prestataire de service de confiance délivre un certificat qualifié est réalisée soit :

1. par la présence en personne de la personne physique ou du représentant autorisé de la personne morale ; ou
2. à distance, à l'aide d'un moyen d'identification électronique pour lequel, avant la délivrance du certificat qualifié, la personne physique ou un représentant autorisé de la personne morale s'est présenté en personne et qui satisfait aux exigences des niveaux de garantie substantiel ou élevé ; ou
3. au moyen d'un certificat de signature électronique qualifié pour une personne physique ou d'un certificat de cachet électronique qualifié pour une personne morale, délivré conformément au point 1 ou 2 ci-dessus ; ou
4. à l'aide d'une autre méthode d'identification reconnue au niveau national fournissant une garantie équivalente en fiabilité à la présence en personne. Cette garantie équivalente est confirmée par un organisme d'évaluation de la conformité.

Note : les informations relatives à l'identité du demandeur et portées dans le certificat électronique doivent correspondre exactement aux informations portées sur les éléments présentés dans le cadre de la vérification d'identité. *Par exemple, pour une personne physique, la troncature du prénom ou du nom, ou l'emploi d'un prénom ou d'un nom ne figurant pas sur l'élément d'identification présenté, ne sont pas acceptables.*

Les paragraphes II.3.1.1 à II.3.1.4 ci-dessous précisent, selon la méthode retenue par le PSCE, les modalités applicables à la vérification de l'identité du demandeur.

II.3.1.1. Exigences applicables à la vérification de l'identité lors d'un face à face

Lors du face à face, la personne physique ou le représentant autorisé de la personne morale doit présenter un document officiel d'identité avec photographie (carte nationale d'identité, passeport, titre de séjour ou autre document relatif au séjour) qui sera vérifié par le personnel du prestataire de services de confiance qualifié. Cette vérification doit permettre d'établir :

- que le visage de la personne physique ou du représentant autorisé de la personne morale correspond à la photographie portée sur le document officiel d'identité présenté ; et
- que ce document est bien dans sa période de validité, et qu'il n'est pas déclaré perdu, volé ou révoqué par une source disponible publiquement ; et
- que ce document ne paraît pas contrefait et ne présente pas de signe de falsification[1].

Pour les organismes publics ou privés délivrant des certificats qualifiés à leurs personnels pour couvrir leurs propres besoins, la preuve d'identité peut également être apportée par la présentation d'une carte d'identité professionnelle avec photographie, ou par la vérification de l'identité du demandeur dans une base de données interne préétablie, comportant la photographie, et dont la constitution repose sur des processus formalisés et audités.

[1] La vérification de l'authenticité d'un document d'identité se fait généralement au moyen d'une inspection physique des caractéristiques de sécurité de ce document. *Parmi les exemples de caractéristiques de sécurité figurent les filigranes, les encres, les hologrammes, la micro-impression, etc.* Le registre en ligne de documents authentiques d'identité et de voyage PRADO (disponible à l'adresse www.consilium.europa.eu/prado/fr) recense les caractéristiques de sécurité des documents d'identité que les Etats membres ont souhaité rendre publiques.

II.3.1.2. Exigences applicables à la vérification de l'identité par le biais d'un moyen d'identification électronique de niveau substantiel ou élevé

Le prestataire de services de confiance qualifié peut accepter les moyens d'identification électroniques :

- ayant fait l'objet d'une notification par l'un des Etats membres de l'Union européenne ; et
- ayant un niveau de garantie substantiel ou élevé ; et
- pour lesquels il est publié une documentation en langue anglaise ou française permettant d'établir, sans ambiguïté, que la présence physique en personne du demandeur est un prérequis à l'obtention de ce moyen d'identification électronique.

II.3.1.3. Exigences applicables à la vérification de l'identité par le biais d'un certificat de signature électronique qualifié ou de cachet électronique qualifié

Un document, relatif à la manifestation du consentement du demandeur pour la délivrance du certificat, doit avoir été signé à l'aide d'une signature électronique avancée reposant sur un certificat qualifié, ou cacheté à l'aide d'un cachet électronique avancé reposant sur un certificat qualifié.

Il est recommandé que ce document soit la demande de certificat déposée électroniquement auprès du prestataire de services de confiance, et comportant l'ensemble des informations nécessaires à la délivrance du certificat.

Le PSCE doit s'assurer que le certificat de signature électronique qualifié ou de cachet électronique qualifié a été délivré selon l'une des deux méthodes décrites aux chapitres III.3.1.1 et III.3.1.2 ci-dessus.

Exemple : un PSCE peut accepter que la vérification d'identité du demandeur lors du premier renouvellement d'un certificat de signature électronique qualifié ou de cachet électronique qualifié puisse être réalisée via le recours au certificat qualifié précédemment délivré par ce PSCE, sous réserve que la vérification d'identité pour la délivrance initiale ait été réalisée conformément aux modalités précisées aux chapitres II.3.1.1 et II.3.1.2. Lors du second renouvellement, en revanche, la vérification de l'identité devra être réalisée selon les mêmes modalités que la délivrance initiale.

Le PSCE doit mettre en œuvre un processus de validation de la signature ou du cachet répondant aux exigences prévues par l'article 32.1 du règlement [eIDAS] (à l'exception du point 32.1.f), appliquées *mutatis mutandis* pour le cachet. Si le PSCE exige une signature qualifiée ou un cachet qualifié, il est recommandé d'avoir recours à un service de validation qualifié des signatures électroniques qualifiées ou des cachets électroniques qualifiés.

Si la création de la signature électronique avancée ou du cachet électronique avancé par le demandeur est mise en œuvre par le biais de moyens fournis par le PSCE, il est recommandé de respecter les bonnes pratiques suivantes :

- le format de la signature ou du cachet électronique est l'un de ceux prévus par les standards référencés dans la décision d'exécution de la Commission [DEC_EXEC_1506] ;
- la signature ou le cachet électronique fait l'objet d'un horodatage qualifié permettant de garantir sa date présumée de création.

II.3.1.4. Autres méthodes d'identification reconnues au niveau national

Le recours à un moyen d'identification électronique de niveau de garantie élevé notifié par l'Etat français permet d'apporter une garantie équivalente à la présence en personne.

D'autres méthodes peuvent être utilisées, sous réserve qu'un organisme d'évaluation de la conformité atteste de leur équivalence, en termes de garantie, avec la présence physique en personne. Cette équivalence devra également être validée par l'ANSSI.

Par exemple, une solution de face-à-face « à distance », où le demandeur fait la preuve de son identité en présentant un document officiel d'identité par le biais d'un système de visio-conférence, pourrait être reconnue comme apportant une équivalence à la présence en personne, sous réserve qu'il soit démontré la mise en place de mesures techniques et organisationnelles permettant de lutter contre les risques de fraude avec une efficacité au moins égale à la présentation physique du document d'identité. Ces mesures devraient notamment couvrir les risques liés à la présentation de documents d'identité falsifiés ou contrefaits, ainsi que les risques liés à la manipulation des dispositifs de capture d'images ou des canaux de communication.

II.3.2. **Compléments relatifs à la constitution et la conservation du dossier de demande**

Pour un certificat qualifié de signature électronique ou d'authentification de site internet, sous la responsabilité d'une personne physique, le dossier d'enregistrement doit au moins comprendre :

- une demande de certificat manuscrite ou électronique datée de moins de 3 mois et signée par le demandeur, comprenant l'ensemble des éléments nécessaires à la délivrance du certificat ;
- les conditions générales d'utilisation, dans leur version en vigueur, signées par le demandeur.

La demande de certificat et les conditions générales d'utilisation doivent être :

- Signées au moyen d'une signature manuscrite ; ou
- Signées électroniquement au moyen d'une signature avancée.

Dans le second cas, il est recommandé que le certificat de signature électronique soit un certificat qualifié.

Pour un certificat qualifié de cachet électronique et d'authentification de site internet, sous la responsabilité d'une personne morale, le dossier d'enregistrement doit au moins comprendre :

- une demande de certificat manuscrite ou électronique datée de moins de 3 mois et signée par un représentant autorisé de la personne morale, comprenant l'ensemble des éléments nécessaires à la délivrance du certificat ;
- les conditions générales d'utilisation, dans leur version en vigueur, datées et signées conformément à la clause 6.3.4 de la norme [EN_319_411-2] ;
- pour une entreprise, toute pièce, valide lors de la demande de certificat, attestant de l'existence de l'entreprise et portant le numéro SIREN de celle-ci, ou, à défaut, une autre pièce attestant l'identification unique de l'entreprise qui figurera dans le certificat ;
- pour une entreprise, tout document attestant de la qualité demandeur de certificat ;
- pour une administration, une pièce, valide au moment de l'enregistrement, portant délégation ou subdélégation de l'autorité responsable de la structure administrative.

La demande de certificat et les conditions générales d'utilisation doivent être :

- Signées au moyen d'une signature manuscrite ; ou
- Signées électroniquement au moyen d'une signature avancée ; ou
- Cachetées électroniquement au moyen d'un cachet avancé.

Dans les deux derniers cas, il est recommandé que le certificat de signature électronique ou de cachet électronique soit un certificat qualifié.

Les dossiers d'enregistrement doivent être conservés pendant sept (7) ans après la fin de validité du certificat faisant l'objet de la demande.

II.3.3. **Compléments relatifs à l'utilisation des systèmes et des produits fiables**

Les modules cryptographiques employés pour signer les certificats des autorités de certification, les certificats des demandeurs, les réponses OCSP et les LCR, et pour générer les clés privées des autorités de certification et les clés privées des demandeurs le cas échéant, doivent respecter les règles spécifiées dans le document [PSCO_QUALIF].

II.3.4. **Compléments relatifs à la suspension des certificats**

La suspension temporaire des certificats qualifiés de signature électronique, de cachet électronique et d'authentification de site internet est interdite.

II.3.5. **Compléments relatifs au statut de révocation des certificats**

Il est recommandé de mettre un œuvre un répondeur OCSP, en particulier si le PSCE émet des certificats d'authentification de site internet. Si le PSCE ne met pas en œuvre de répondeur OCSP, alors il doit assurer la publication d'une LCR.

Dans le cas où le PSCE met à disposition le statut de révocation des certificats à la fois via la publication d'une LCR et la mise en œuvre d'un répondeur OCSP, la norme [EN_319_411-2] prévoit une cohérence, sur la durée, des informations fournies par ces deux moyens. Le respect de cette exigence ne doit pas empêcher un répondeur OCSP d'utiliser le statut « *unknown* » ou « *revoked* » en cas de requête portant sur un certificat non connu, conformément au chapitre 2.2 de la [RFC_6960].

II.3.6. **Compléments relatifs à l'accessibilité du statut de révocation au-delà de la fin de validité**

Le PSCE doit assurer la disponibilité du statut de révocation à tout moment et au-delà de la période de validité du certificat.

Afin de répondre à cette exigence, il est recommandé d'appliquer les règles suivantes, selon le cas :

1) Après l'expiration du certificat qualifié :
    a. si le PSCE assure la publication d'une LCR, celle-ci devrait :
        i. comporter l'extension « *ExpiredCertsOnCRL* », comme prévu par la recommandation ITU-T X.509 ; et
        ii. contenir les numéros de série de l'ensemble des certificats révoqués, y compris les certificats étant arrivés à expiration après leur révocation.
    b. si le PSCE met en œuvre un répondeur OCSP, celui-ci devrait :
        i. comporter l'extension « *archive cutoff* », comme prévu par la RFC 6960, avec une date identique à la date de début de validité du certificat de l'AC ; et
        ii. maintenir disponible le statut de révocation du certificat après son expiration.

2) Si la clé de l'AC émettrice du certificat qualifié est sur le point d'expirer :
    a. l'ensemble des certificats non-expirés émis par cette AC devraient être révoqués ; et
    b. si le PSCE assurait la publication d'une LCR, une dernière LCR devrait être publiée, celle-ci ayant une fin de validité positionnée au 31 décembre 9999, 23h59m59s (« *99991231235959Z* »); et
    c. si le PSCE assurait un service de répondeur OCSP, une dernière réponse OCSP devrait être pré-générée pour chaque certificat émis, cette réponse ayant une fin de validité positionnée au 31 décembre 9999, 23h59m59s (« *99991231235959Z* »).

3) Lorsque le PSCE cesse de fournir le service de confiance qualifié, sans le transférer vers un autre PSCE qualifié :
    a. les méthodes applicables au cas n°2 sont applicables dans ce cas ; et
    b. le PSCE n'est pas tenu de maintenir la publication des LCR ni de maintenir le service OCSP, mais les LCR et/ou réponses OCSP produites devraient être mises à disposition des clients du PSCE dans des conditions permettant de garantir leur intégrité.

Dans tous les cas, le PSCE doit rendre publique les mesures mises en œuvre pour répondre à l'exigence.

II.3.7. **Compléments relatifs à la crypto-période des clés privées**

Les bi-clés doivent être périodiquement renouvelées afin de minimiser les possibilités d'attaques cryptographiques.

Il est recommandé que la durée de vie des bi-clés correspondant aux certificats qualifiés de signature électronique, de cachet électronique et d'authentification internet n'excède pas les durées indiquées dans le tableau suivant :

Type de certificat	**Durée maximale de validité**
Signature électronique (Personne physique)	La durée maximale de validité doit être fonction de la taille de clé, conformément aux règles de la clause 9.3 du standard [TS_119_312]. La durée maximale recommandée est de 3 ans.
Cachet électronique (Personne morale)	
Authentification internet (Personne physique ou Personne morale)	La durée maximale de validité est de 27 mois. La durée maximale recommandée est de 1 an.

II.3.8. **Compléments relatifs à la durée de validité des certificats**

La durée de validité d'un certificat qualifié ne peut excéder la durée de validité restante du certificat de l'autorité de certification émettrice.

II.3.9. **Compléments relatifs au cumul des usages de clés**

Il est recommandé d'appliquer les règles suivantes :

- les certificats qualifiés de signature électronique devraient contenir l'usage de clé *nonRepudiation* (aussi appelé *contentCommitment*) à l'exclusion de tout autre ;
- les certificats qualifiés de cachet électronique devraient contenir les usages de clés *digitalSignature* et/ou *nonRepudiation* à l'exclusion de tout autre ;
- les certificats qualifiés d'authentification de site internet devraient contenir les usages de clés *digitalSignature* et/ou *keyEncipherment*, ou *keyAgreement*, à l'exclusion de tout autre.

Annexes

I. Annexe 1 Références documentaires

Renvoi	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
[EN_319_411-2]	ETSI EN 319 411-2 V2.1.1 (2016-02) : Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.
[EN_319_412-1]	ETSI EN 319 412-1 V1.1.1 (2016-02) : Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures. Disponible sur : http://www.etsi.org
[EN_319_412-5]	ETSI EN 319 412-5 V2.1.1 (2016-02) : Part 5: QCStatements.
[NOTIFICATION]	Note des autorités française du 17 février 2015 à la Commission, désignant l'ANSSI comme organe de contrôle au titre du règlement eIDAS.
[PSCE_RGS_EIDAS]	Services de délivrance de certificats qualifiés de signature électronique, de cachet électronique et d'authentification de site internet - Modalités de qualification selon le règlement eIDAS des services qualifiés selon le RGS, version en vigueur. 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
[RFC_5280]	Internet Engineering Task Force (IETF) - Request for Comments : 5280 X.509 Internet Public Key Infrastructure. Certificate and Certificate Revocation List (CRL) Profile.
[RFC_6960]	Internet Engineering Task Force (IETF) - Request for Comments : 6960 X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol – OCSP.
[RGS]	Référentiel général de sécurité, version en vigueur. Disponible sur http://www.ssi.gouv.fr
[TS_119_312]	ETSI TS 119 312 V1.1.1 (2014-11) : Electronic Signatures and Infrastructures (ESI); Cryptographic Suites. Disponible sur : http://www.etsi.org

II. Annexe 2 Profils de certificats recommandés

Les tableaux suivants présentent quatre types de profils de certificats permettant d'apporter une présomption de conformité aux exigences du règlement. Il est recommandé aux PSCE de respecter ces profils de certificats. Dans le cas contraire, le PSCE doit démontrer le respect des exigences applicables des annexes I, III et IV du règlement [eIDAS].

Par exemple, un PSCE pourrait, pour les certificats de signature électronique qu'il émet, ne pas utiliser les attributs givenName et surname pour identifier ses porteurs, et utiliser uniquement l'attribut commonName. Dans ce cas, la structure du commonName doit permettre d'identifier sans ambiguïté le nom du demandeur du certificat.

Les certificats peuvent contenir d'autres champs ou extensions que ceux définis ci-dessous, en conformité avec la [RFC 5280].

II.1.Socle commun à tous les profils de certificats

<table>
<tr><th>Champ</th><th>Valeur</th></tr>
<tr><td>Version</td><td>2 (=version 3).</td></tr>
<tr><td>Serial number</td><td>Unique pour chaque certificat généré au sein du domaine d'une AC.</td></tr>
<tr><td>Signature Algorithm</td><td>Algorithme de signature conforme aux règles de la note [PSCO_QUALIF].</td></tr>
<tr><td>Issuer</td><td>
<table>
<tr><th>Attribut</th><th>Valeur</th></tr>
<tr><td>countryName</td><td>Nom du pays de l'autorité compétente auprès de laquelle le prestataire est officiellement enregistré (tribunal de commerce, ministère, …).</td></tr>
<tr><td>organizationName</td><td>Nom officiel complet du prestataire tel qu'enregistré auprès des autorités compétentes[2].</td></tr>
<tr><td>organizationIdentifier</td><td>Numéro d'immatriculation officiel du prestataire conformément à [EN_319_412-1] clause 5.1.4.
En France, ce numéro d'immatriculation peut également être constitué du préfixe « SI:FR- » suivi du numéro SIREN ou SIRET.</td></tr>
<tr><td>commonName</td><td>Nom significatif du prestataire ou du service de délivrance de certificats.</td></tr>
</table>
</td></tr>
<tr><td>Not Before</td><td>Date de début de validité du certificat, conformément aux règles des chapitres II.3.7 et II.3.8.</td></tr>
<tr><td>Not After</td><td>Date de fin de validité du certificat, conformément aux règles des chapitres II.3.7 et II.3.8.</td></tr>
<tr><td>Subject</td><td>Voir les règles applicables à chaque type de certificat, dans les annexes II.2, II.3 et II.4.</td></tr>
<tr><td>Public Key Algorithm</td><td>Algorithme de clé publique conforme aux règles de la note [PSCO_QUALIF].</td></tr>
<tr><td>Public-Key</td><td>Clé publique.</td></tr>
</table>

[2] A titre dérogatoire, une représentation non ambigüe du nom officiel du prestataire peut également être utilisée (*par exemple, une abréviation reconnue et largement utilisée du nom officiel).*

<table>
<tr><th>Extension</th><th>Obligatoire</th><th>Critique</th><th>Valeur</th></tr>
<tr><td>Basic Constraints</td><td>Oui</td><td>Non</td><td>“CA:false”.</td></tr>
<tr><td>Certificate Policies</td><td>Oui</td><td>Non</td><td>Identifiant de la Politique de Certification applicable.</td></tr>
<tr><td>CRL Distribution Points</td><td>Conditionnel</td><td>Non</td><td>Point de publication des listes de certificats révoqués.
En cas d’absence d’un service OCSP :
• un point de distribution des LCR est requis ;
• le point de publication des LCR doit faire référence à une LCR publiée.
Au moins une des LCR publiées doit être accessible selon le protocole http ou LDAP.</td></tr>
<tr><td>Authority Information Access</td><td>Oui</td><td>Non</td><td>Renseignement de l’extension « Authority Information Access » :
• accessMethod OID valorisé à « id-ad-caIssuers » ;
• accessLocation valorisé avec le chemin d’accès au certificat de l’AC (URL http de téléchargement du certificat de l’AC).
En complément, si un répondeur OCSP est mis en œuvre :
• accessMethod OID valorisé à « id-ad-ocsp » ;
• accessLocation valorisé avec le chemin d’accès au répondeur OCSP (obligatoire si aucune LCR n’est publiée).</td></tr>
<tr><td>Key Usage</td><td>Oui</td><td>Oui</td><td>Voir les règles applicables à chaque type de certificat, dans les annexes II.2, II.3 et II.4.</td></tr>
<tr><td>qcStatements</td><td>Oui</td><td>Non</td><td>
<table>
<tr><th>Extension</th><th>Présente</th><th>Commentaire</th></tr>
<tr><td>esi4-qcStatement-1</td><td>Oui</td><td>Indication que le certificat émis est qualifié, via la valeur “ id-etsi-qcs-QcCompliance”.</td></tr>
<tr><td>esi4-qcStatement-2</td><td>Opt.</td><td>Extension optionnelle, décrite dans la norme [EN_319_ 412-5].</td></tr>
<tr><td>esi4-qcStatement-3</td><td>Opt.</td><td>Extension optionnelle, décrite dans la norme [EN_319_ 412-5].</td></tr>
<tr><td>esi4-qcStatement-4</td><td>Cond.</td><td>Voir les règles applicables à chaque type de certificat, dans les annexes II.2, II.3 et II.4.</td></tr>
<tr><td>esi4-qcStatement-5</td><td>Opt.</td><td>Extension optionnelle, décrite dans la norme [EN_319_ 412-5].</td></tr>
<tr><td>esi4-qcStatement-6</td><td>Oui</td><td>Voir les règles applicables à chaque type de certificat, dans les annexes II.2, II.3 et II.4.</td></tr>
</table>
</td></tr>
<tr><td>Subject Alternative Name</td><td>Conditionnel</td><td>Non</td><td>Voir les règles applicables à chaque type de certificat, dans les annexes II.2, II.3 et II.4.</td></tr>
<tr><td>Subject Key Identifier</td><td>Oui</td><td>Non</td><td>Identifiant de la clé publique contenue dans le certificat.</td></tr>
<tr><td>Authority Key Identifier</td><td>Oui</td><td>Non</td><td>Identifiant de la clé publique de l'AC émettrice.</td></tr>
</table>

II.2.Compléments relatifs aux certificats qualifiés de signature électronique

<table>
<tr><th>Champ</th><th>Valeur</th></tr>
<tr><td>Subject</td><td>
<table>
<tr><th>Attribut</th><th>Valeur</th></tr>
<tr><td>countryName</td><td>Nom de pays, spécifiant le contexte général dans lequel les autres attributs doivent être interprétés. Le PSCE doit expliquer dans sa politique de certification la valorisation de cet attribut.</td></tr>
<tr><td>organizationName</td><td>(Obligatoire si le certificat est délivré au porteur dans le cadre de son appartenance à une entité donnée, interdit sinon) Nom officiel complet de l’entité dont dépend le porteur tel qu'enregistré auprès des autorités compétentes.</td></tr>
<tr><td>organizationIdentifier</td><td>(Obligatoire si le certificat est délivré au porteur dans le cadre de son appartenance à une entité donnée, interdit sinon) Numéro d’immatriculation officiel de l’entité dont dépend le porteur conformément à [EN_319_412-1] clause 5.1.4.
En France, ce numéro d’immatriculation peut également être constitué du préfixe « SI:FR- » suivi du numéro SIREN ou SIRET.</td></tr>
<tr><td>serialNumber</td><td>(Optionnel) Elément complémentaire permettant de distinguer les homonymes.</td></tr>
</table>
En cas d’utilisation de l’état civil du porteur :
<table>
<tr><th>Attribute</th><th>Value</th></tr>
<tr><td>givenName</td><td>Prénom usuel ou prénoms de l’état civil du porteur.</td></tr>
<tr><td>surname</td><td>Nom de l'état civil ou nom d’usage du porteur.</td></tr>
<tr><td>commonName</td><td>Nom complet du porteur tel qu’il devrait être affiché par les applications. Il est recommandé d’indiquer le prénom usuel, suivi d'un espace, suivi du nom de l'état civil ou, le cas échéant, du nom d’usage du porteur.</td></tr>
</table>
Ou, en cas d’utilisation d’un pseudonyme :
<table>
<tr><th>Attribute</th><th>Value</th></tr>
<tr><td>Pseudonym</td><td>Pseudonyme du porteur.</td></tr>
<tr><td>commonName</td><td>Pseudonyme du porteur.</td></tr>
</table>
</td></tr>
</table>

Extension	Obligatoire	Critique	Valeur
Key Usage	Oui	Oui	Usage de clé conformes au chapitre II.3.9 du présent document : *nonRepudiation.*
qcStatements	Oui	Non	<table><tr><th>Extension</th><th>Présente</th><th>Commentaire</th></tr><tr><td>esi4-qcStatement-4</td><td>Cond.</td><td>Indication que la clé privée correspondante est stockée dans un dispositif sécurisé de création de signature électronique. Valeur “ *id-etsi-qcs-QcSSCD*”.</td></tr><tr><td>esi4-qcStatement-6</td><td>Oui</td><td>Indication que le certificat est un certificat qualifié de signature électronique. Valeur “*id-etsi-qct-esign*”.</td></tr></table>
Subject Alternative Name	Non	Non	*Cette extension ne devrait pas être présente.*

II.3.Compléments relatifs aux certificats qualifiés de cachet électronique

Field	Value	
Subject	Attribute	Value
	countryName	Nom du pays de l'autorité compétente auprès de laquelle l'entité responsable du certificat est officiellement enregistrée (*tribunal de commerce, ministère, …*).
	organizationIdentifier	Numéro d'immatriculation officiel de l'entité responsable du certificat conformément à [EN_319_412-1] clause 5.1.4. En France, ce numéro d'immatriculation peut également être constitué du préfixe « SI:FR- » suivi du numéro SIREN ou SIRET.
	organizationName	Nom officiel complet de l'entité responsable du certificat, tel qu'enregistré auprès des autorités compétentes.
	commonName	Nom significatif du service mettant en œuvre le cachet.

Extension	Obligatoire	Critique	Valeur
Key Usage	Oui	Oui	Usages de clé conformes au chapitre II.3.9 du présent document : *digitalSignature* et/ou *nonRepudiation.*
qcStatements	Oui	Non	**Extension** / **Présente** / **Commentaire** esi4-qcStatement-4 / Cond. / Indication que la clé privée correspondante est stockée dans un dispositif sécurisé de création de signature électronique. Valeur " *id-etsi-qcs-QcSSCD*". esi4-qcStatement-6 / Oui / Indication que le certificat est un certificat qualifié de signature électronique. Valeur "*id-etsi-qct-eseal*".
Subject Alternative Name	Non	Non	*Cette extension ne devrait pas être présente.*

II.4.Compléments relatifs aux certificats qualifiés d'authentification de site internet ¨

<table>
<tr><th>Field</th><th>Value</th></tr>
<tr><td>Subject</td><td>
<table>
<tr><th>Attribute</th><th>Value</th></tr>
<tr><td>countryName</td><td>Pays dans lequel est établi ou réside le demandeur</td></tr>
<tr><td>localityName</td><td>Ville dans laquelle est établi ou réside le demandeur.</td></tr>
<tr><td>organizationName</td><td>(Obligatoire si le demandeur est une personne morale, ou si le certificat est délivré à une personne physique dans le cadre de son appartenance à une entité donnée, absent sinon) Nom officiel complet de l'entité tel qu'enregistré auprès des autorités compétentes.</td></tr>
<tr><td>organizationIdentifier</td><td>(Obligatoire si le demandeur est une personne morale, ou si le certificat est délivré à une personne physique dans le cadre de son appartenance à une entité donnée, absent sinon) Numéro d'immatriculation officiel de l'entité conformément à [EN_319_412-1] clause 5.1.4.
En France, ce numéro d'immatriculation peut également être constitué du préfixe « SI:FR- » suivi du numéro SIREN ou SIRET.</td></tr>
<tr><td>commonName</td><td>(Optionnel) L'un des noms de domaine présents dans l'extension SubjectAltname.</td></tr>
</table>
Si le certificat a été délivré à une personne physique identifiée par son état civil :
<table>
<tr><th>Attribute</th><th>Value</th></tr>
<tr><td>givenName</td><td>Prénom usuel ou prénoms de l'état civil du demandeur.</td></tr>
<tr><td>surname</td><td>Nom de l'état civil ou nom d'usage du demandeur.</td></tr>
<tr><td>serialNumber</td><td>(Optionnel) Elément complémentaire permettant de distinguer les homonymes.</td></tr>
</table>
Si le certificat a été délivré à une personne physique identifiée par un pseudonyme :
<table>
<tr><th>Attribute</th><th>Value</th></tr>
<tr><td>Pseudonym</td><td>Pseudonyme du demandeur.</td></tr>
<tr><td>surname</td><td>Nom de l'état civil ou le nom d'usage du demandeur.</td></tr>
<tr><td>serialNumber</td><td>(Optionnel) Elément complémentaire permettant de distinguer les homonymes.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Extension</th><th>Obligatoire</th><th>Critique</th><th>Valeur</th></tr>
<tr><td>Key Usage</td><td>Oui</td><td>Oui</td><td>Usages de clé conformes au chapitre II.3.9 du présent document : digitalSignature et/ou keyEncipherment, ou keyAgreement</td></tr>
<tr><td>qcStatements</td><td>Oui</td><td>Non</td><td>
<table>
<tr><th>Extension</th><th>Présente</th><th>Commentaire</th></tr>
<tr><td>esi4-qcStatement-4</td><td>Non</td><td>Cette extension ne devrait pas être présente.</td></tr>
<tr><td>esi4-qcStatement-6</td><td>Oui</td><td>Indication que le certificat est un certificat qualifié d'authentification de site internet.
Valeur "id-etsi-qct-web".</td></tr>
</table>
</td></tr>
<tr><td>Subject Alternative Name</td><td>Oui</td><td>Non</td><td>Un ou plusieurs noms de domaine contrôlés par le demandeur.</td></tr>
</table>

III. Annexe 3 Couverture des exigences du règlement [eIDAS]

Article	Exigence du règlement eIDAS	Clauses applicables des normes européennes	Chapitres applicables du présent document
24(1)	Vérification de l'identité et des attributs spécifiques de la personne physique ou morale	[EN_319_411-2] clause 6.2.2 et 6.2.3	II.3.1
24(2).e	Utilisation des systèmes et des produits fiables	[EN_319_411-2] clause 6.5	II.3.3
24(2).h	Conservation des informations délivrées et reçues par le prestataire de services de confiance	[EN_319_411-2] Clauses 6.4.5 et 6.4.6	II.3.2
24(2).i	Continuité de service suite à l'arrêt d'activité du prestataire de services de confiance	[EN_319_411-2] clause 6.4.9	II.3.2
24(2).k	Base de données relative aux certificats émis	[EN_319_411-2] clause 6.1	*Pas de complément à la norme*
24(3)	Révocation du certificat	[EN_319_411-2] clause 6.2.4	II.3.4 et II.3.5
24(4)	Accès fiable, gratuit et efficace au statut de révocation du certificat	[EN_319_411-2] clause 6.3.10	II.3.6
28(1)	Certificats qualifiés de signature électronique	[EN_319_411-2] clause 6.6.1	Annexe II (et chapitres II.3.7 à II.3.9)
38(1)	Certificats qualifiés de cachet électronique		
45(1)	Certificats qualifiés d'authentification de site internet		
28(4) 38(4)	Aspect relatifs à la révocation	[EN_319_411-2] clause 6.3.9	II.3.5
28(5) 38(5)	Aspects relatifs à la suspension	[EN_319_411-2] clause 6.3.9	II.3.4