CRITÈRES D'ÉVALUATION DE LA CONFORMITÉ AU RÉFÉRENTIEL GÉNÉRAL DE SÉCURITÉ DES SERVICES DE DÉLIVRANCE DE CERTIFICATS QUALIFIÉS DE SIGNATURE ÉLECTRONIQUE, DE CACHET ÉLECTRONIQUE ET D'AUTHENTIFICATION DE SITE INTERNET

Annexe à l'arrêté ministériel n° 2018-68
du 30 janvier 2018

ANNEXE AU « JOURNAL DE MONACO » N° 8.368

DU 9 FÉVRIER 2018

SOMMAIRE

1. Introduction....2

1.1. Objet....2

1.2. Mise à jour....3

1.3. Liste des abréviations....3

2. Exigences relatives aux services de délivrance de certificats qualifiés....3

2.1. Modalités de qualification....3

2.1.1. Processus de qualification....3

2.1.2. Inscription à la liste de confiance..3

2.2. Critères d'évaluation de la conformité....4

2.3. Compléments à la norme européenne ETSI [EN_319_411-2]....4

2.3.1. Compléments relatifs à la vérification de l'identité du demandeur....6

2.3.2. Compléments relatifs à la constitution et la conservation du dossier de demande....6

2.3.3. Compléments relatifs à l'utilisation des systèmes et des produits fiables....6

2.3.4. Compléments relatifs à la suspension des certificats....6

2.3.5. Compléments relatifs au statut de révocation des certificats....6

2.3.6. Compléments relatifs à l'accessibilité du statut de révocation au-delà de la fin de validité....7

2.3.7. Compléments relatifs à la crypto-période des clés privées...7

2.3.8. Compléments relatifs à la durée de validité des certificats....7

2.3.9. Compléments relatifs au cumul des usages de clés....8

Appendice 1 : Références documentaires....8

Appendice 2 : Profils de certificats recommandés....9

1) Socle commun à tous les profils de certificats 13

2) Compléments relatifs aux certificats qualifiés de signature électronique 15

3) Compléments relatifs aux certificats qualifiés de cachet électronique 16

4) Compléments relatifs aux certificats qualifiés d'authentification de site internet 17

---

1. Introduction

1.1. Objet

Conformément à l'Ordonnance Souveraine n° 5.664 du 23 décembre 2015, modifiée, susvisée, l'Agence Monégasque de Sécurité Numérique est l'autorité nationale en charge de la sécurité des systèmes d'information.

Elle est, en outre, l'organe de contrôle de la Principauté pour les prestataires de services de confiance et les services de confiance ayant notamment pour mission, de procéder à des contrôles aux fins de vérifier que lesdits prestataires et les services de confiance qualifiés qu'ils fournissent respectent les exigences du Référentiel Général de Sécurité, annexé à l'arrêté ministériel n° 2017-835 du 29 novembre 2017, susvisé, de vérifier l'existence des plans d'arrêt des services de confiance qualifiés et leur mise en œuvre effective ainsi que d'établir et tenir à jour la liste de confiance prévue au paragraphe 26 dudit référentiel.

La présente annexe décrit, dans le respect des règles posées par le Référentiel Général de Sécurité, précité, les critères d'évaluation de la conformité 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 l'annexe à l'arrêté ministériel n° 2018-66 du 30 janvier 2018, susvisé, [PSCO_QUALIF] applicables à l'ensemble des prestataires de services de confiance qualifiés.

Seul le respect, par les services de délivrance de certificats qualifiés de signature électronique, de cachet électronique et d'authentification de site internet, mis en œuvre par un prestataire de services de confiance, des exigences générales déclinées au chapitre 2, permet de donner plein effet aux règles posées par le Référentiel Général de Sécurité, précité, en ce qui concerne les exigences respectives de ses appendices I, III, IV.

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, permettant de donner plein effet aux dispositions de l'article 3 de l'Ordonnance Souveraine n° 6.525 du 16 août 2017, susvisée.

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, permettant de donner plein effet aux règles posées au paragraphe 37 du Référentiel Général de Sécurité, précité.

1.2. Mise à jour

La mise à jour de la présente annexe est réalisée par l'Agence Monégasque de Sécurité Numérique en fonction des évolutions législatives et règlementaires en matière de sécurité des systèmes d'information. Ladite de mise à jour est publiée par arrêté ministériel, lequel précise les modalités de transition et date d'effet.

1.3. Liste des abréviations

Les abréviations utilisées dans la présente annexe sont les suivantes :

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
PSCE	Prestataires de Services de Certification Electronique
RGS	Référentiel Général de Sécurité
QSCD	Qualified electronic Signature / Seal Creation Device (dispositif de création de signature qualifiée)
AC	Autorité de Certification émettant des certificats pour un usage déterminé
LCR	Liste des Certificats Révoqués
OCSP	Online Certificate Status Protocol (protocole de vérification de certificat en ligne)
OID	Object IDentifier (identifiants universels)
URL	Uniform Resource Locator (localisateur uniforme de ressource)
http	hypertext transfer protocol (protocole de transfert hypertexte)
LDAP	Lightweight Directory Access Protocol (protocole d'accès au répertoire allégé)
RCI	Répertoire du Commerce et de l'Industrie
UIT	Union Internationale des Télécommunications
IETF	Groupe de travail international d'ingénierie de l'Internet

2. Exigences relatives aux services de délivrance de certificats qualifiés

2.1. Modalités de qualification

2.1.1. 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 l'annexe à l'arrêté ministériel n° 2018-66 du 30 janvier 2018, précité [PSCO_QUALIF].

2.1.2. Inscription à la liste de confiance

Un service de délivrance de certificats qualifiés est identifié dans la liste de confiance visée au paragraphe 26 du Référentiel Général de Sécurité, précité, 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).

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.

2.2. Critères d'évaluation de la conformité

L'évaluation doit permettre de démontrer le respect des exigences du Référentiel Général de Sécurité, précité, applicables aux services de délivrance de certificats qualifiés de signature électronique, de cachet électronique et d'authentification de site internet, spécifiées dans les paragraphes suivants dudit référentiel :

• Pour les prestataires de services de confiance qualifiés délivrant des certificats qualifiés :

- 23(1) Vérification de l'identité et des attributs spécifiques de la personne physique ou morale ;
- 23(2).e Utilisation de systèmes et des produits fiables, sécurité et fiabilité des processus ;
- 23(2).h Conservation des informations délivrées et reçues dans le cadre de la délivrance des certificats qualifiés ;
- 23(2).i Continuité de service suite à l'arrêt d'activité de délivrance de certificats qualifiés ;
- 23(2).k Base de données relative aux certificats émis ;
- 23(3) Révocation des certificats ;
- 23(4) Accès fiable, gratuit et efficace au statut de révocation des certificats.

• Pour les certificats qualifiés :

- 30(1) Certificats qualifiés de signature électronique ;
- 30(3) Autorisation d'attributs spécifiques complémentaires non obligatoires ;
- 30(4) Aspect relatifs à la révocation de ces certificats ;
- 30(5) Aspects relatifs à la suspension de ces certificats ;
- 40(1), (3), (4), (5) Certificats qualifiés de cachet électronique, aspects relatifs à la révocation et suspension de ces certificats ;
- 45(1) Certificats qualifiés d'authentification de site Internet.

Le respect des exigences de la norme européenne ETSI [EN 319 411-2] et des compléments précisés dans le chapitre 2.3, permet d'apporter une présomption de conformité à ces exigences.

2.3. Compléments à la norme européenne ETSI [EN_319_411-2]

2.3.1. 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 ; 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.

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 2.3.1.1 à 2.3.1.4 précisent, selon la méthode retenue par le PSCE, les modalités applicables à la vérification de l'identité du demandeur.

2.3.1.1. 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 ; 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.

2.3.1.2. 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 États membres de l'Union européenne, et
- ayant un niveau de garantie substantiel ou élevé, et
- pour lesquels il existe 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.

2.3.1.3. 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 comporte 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 2.3.1.1 et 2.3.1.2.

Le PSCE doit mettre en œuvre un processus de validation de la signature ou du cachet répondant aux exigences prévues au paragraphe 34.1 de l'annexe à l'arrêté ministériel n° 2017-835 du 29 novembre 2017, précité, (à l'exception du point 34.1.f). 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 européenne n° 2015/1506 en date du 8 septembre 2015 [DEC_EXEC_1506] ;
- la signature ou le cachet électronique fait l'objet d'un horodatage qualifié permettant de garantir sa date présumée de création.

2.3.1.4. Autres méthodes d'identification reconnues au niveau national

Le recours à un moyen d'identification électronique de niveau de garantie élevé notifié par l'État Monégasque est reconnu comme apportant 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'Agence Monégasque de Sécurité Numérique.

---

[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 États membres de l'Europe ont souhaité rendre publiques.

2.3.2. 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 signée, et datée de moins de trois (3) mois, par le demandeur, et 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 trois (3) mois, signée par un représentant autorisé de la personne morale et 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 européenne [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 son numéro d'immatriculation au répertoire du commerce et de l'industrie, 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 du demandeur de certificat ;
- pour une administration, une pièce, valide au moment de l'enregistrement, portant délégation de signature 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.

2.3.3. Compléments relatifs à l'utilisation des systèmes et des produits fiables

Les modules cryptographiques employés d'une part pour signer les certificats des autorités de certification, les certificats des demandeurs, les réponses OCSP ainsi que les LCR, et d'autre part pour générer les clés privées des autorités de certification et les clés privées des demandeurs le cas échéant, doivent respecter les règles spécifiées dans l'arrêté ministériel n° 2018-66 du 30 janvier 2018, précité [PSCO_QUALIF].

2.3.4. 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.

2.3.5. 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 européenne ETSI [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 du document [RFC_6960] émanant du groupe de travail international d'ingénierie sur internet, l'IETF.

2.3.6. 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, émanant de l'Union Internationale des Communications, l'UIT ; 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 le document, [RFC_6960], précité, 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.

2.3.7. 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 ETSI [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.

2.3.8. 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.

2.3.9. 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.

Appendice 1 : Références documentaires

[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]

[EN_319_411-2] Norme européenne 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] Norme européenne 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

[PSCO_QUALIF] Arrêté ministériel n° 2018-66 du 30 janvier 2018 portant application de l'arrêté ministériel n° 2017-835 du 29 novembre 2017 portant application l'article 54 de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, relatif aux critères d'évaluation de la conformité au règlement général de sécurité des prestataires de services de confiance qualifiés

[RFC_5280] Document Internet Engineering Task Force (IETF) - Request for Comments : 5280

X.509 Internet Public Key Infrastructure

Certificate and Certificate Revocation List (CRL) Profile

[RFC_6960] Document 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, annexe à l'arrêté ministériel n° 2017-835 du 29 novembre 2017 portant application l'article 54 de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré
[TS_119_312]	Standard ETSI TS 119 312 V1.1.1 (2014-11) : Electronic Signatures and Infrastructures (ESI); Cryptographic Suites. Disponible sur : http://www.etsi.org
[ITU-T X.509]	Recommandation UIT-T X.509 | ISO/CEI 9594-8 qui définit des cadres pour l'infrastructure de clé publique (PKI) et l'infrastructure de gestion de privilège (PMI)

Appendice 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 Référentiel Général de Sécurité, précité.

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

1) Socle commun à tous les profils de certificats

Champ	Valeur
Version	2 (=version 3)
Serial number	Unique pour chaque certificat généré au sein du domaine d'une AC
Signature Algorithm	Algorithme de signature conforme aux règles de l'arrêté [PSCO_QUALIF]
Issuer	countryName : Nom du pays de l'autorité compétente auprès de laquelle le prestataire est officiellement enregistré (tribunal de commerce, ministère,…) organizationName : Nom officiel complet du prestataire tel qu'enregistré auprès des autorités compétentes[2] organizationIdentifier : Numéro d'immatriculation officiel du prestataire conformément à [EN_319_412-1] clause 5.1.4. À Monaco, ce numéro d'immatriculation peut également être constitué du préfixe « SI:MC- » suivi du numéro RCI commonName : Nom significatif du prestataire ou du service de délivrance de certificats
Not Before	Date de début de validité du certificat, conformément aux règles des chapitres 2.3.7, 2.3.8 et 2.3.9
Not After	Date de fin de validité du certificat, conformément aux règles des chapitres 2.3.7, 2.3.8 et 2.3.9
Subject	*Voir les règles applicables à chaque type de certificat, dans l'annexe II 2), 3) et 4)*
Public Key Algorithm	Algorithme de clé publique conforme aux règles de l'arrêté [PSCO_QUALIF]
Public-Key	Clé publique

[2] À 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 colspan="3">Valeur</th></tr>
<tr><td>Basic Constraints</td><td>Oui</td><td>Non</td><td colspan="3">« CA : false »</td></tr>
<tr><td>Certificate Policies</td><td>Oui</td><td>Non</td><td colspan="3">Identifiant de la Politique de Certification applicable</td></tr>
<tr><td>CRL Distribution Points</td><td>Conditionnel</td><td>Non</td><td colspan="3">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 colspan="3">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 colspan="3">Voir les règles applicables à chaque type de certificat, dans les annexes II.2, II.3 et II.4.</td></tr>
<tr><td rowspan="3">qcStatements</td><td rowspan="3">Oui</td><td rowspan="3">Non</td><td>Extension</td><td>Présente</td><td>Commentaire</td></tr>
<tr><td>Esi4-qcStatement-1</td><td>Oui</td><td>Indication de 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>
</table>

			Esi4-qcStatement-3	Opt.	Extension optionnelle, décrite dans la norme [EN_319_412-5]
			Esi4-qcStatement-4	Cond.	*Voir les règles applicables à chaque type de certificat, dans l'annexe II 2), 3) et 4)*
			Esi4-qcStatement-5	Opt.	Extension optionnelle, décrite dans la norme [EN_319_412-5]
			Esi4-qcStatement-6	Oui	*Voir les règles applicables à chaque type de certificat, dans l'annexe II 2), 3) et 4)*
Subject Alternative Name	Conditionnel	Non	*Voir les règles applicables à chaque type de certificat, dans l'annexe II 2), 3) et 4)*		
Subject Key Identifier	Oui	Non	Identifiant de la clé publique contenue dans le certificat		
Authority Key Identifier	Oui	Non	Identifiant de la clé publique de l'AC émettrice		

2) Compléments relatifs aux certificats qualifiés de signature électronique

Champ	**Valeur**	
Subject	**Attribut**	**Valeur**
	countryName	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
	organizationName	*(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

	organizationIdentifier	*(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 la norme européenne ETSI [EN_319_412-1] clause 5.1.4 À Monaco, ce numéro d'immatriculation peut également être constitué du préfixe « SI:MC- » suivi du numéro RCI
	serialNumber	*(Optionnel)* Élément complémentaire permettant de distinguer les homonymes
	En cas d'utilisation de l'état civil du porteur	
	Attribute	**Value**
	givenName	Prénom usuel ou prénoms de l'état civil du porteur
	surname	Nom de l'état civil ou nom d'usage du porteur
	commonName	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
	Ou, en cas d'utilisation d'un pseudonyme	
	Attribute	**Value**
	Pseudonym	pseudonyme du porteur
	commonName	pseudonyme du porteur

Extension	Obligatoire	Critique	Valeur
Key Usage	Oui	Oui	Usages de clé conformes au chapitre 2.3.9 du présent document : nonRepudiation
Subject Alternative Name	Non	Non	*Cette extension ne devrait pas être présente*

QCStatements	Oui	Non			
			Extension	**Présente**	**Commentaire**
			esi4-qcStatement-4	Cond.	Indique 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	Valeur « id-etsi-qct-esign » Indication que le certificat est un certificat qualifié de signature électronique

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 le prestataire est officiellement enregistré *(tribunal de commerce, ministère,…)*
	organizationIdentifier	Numéro d'immatriculation officiel de l'entité responsable du certificat conformément à la norme européenne ETSI [EN_319_412- 1] clause 5.1.4 À Monaco, ce numéro d'immatriculation peut également être constitué du préfixe « SI:MC- » suivi du numéro RCI
	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

<table>
<tr><th>Extension</th><th>Obligatoire</th><th>Critique</th><th colspan="3">Valeur</th></tr>
<tr><td>Key Usage</td><td>Oui</td><td>Oui</td><td colspan="3">Usages de clé conformes au chapitre 2.3.9 du présent document : nonRepudiation</td></tr>
<tr><td>Subject Alternative Name</td><td>Non</td><td>Non</td><td colspan="3">Cette extension ne devrait pas être présente</td></tr>
<tr><td rowspan="3">QCStatements</td><td rowspan="3">Oui</td><td rowspan="3">Non</td><td colspan="3"></td></tr>
<tr><td>Extension</td><td>Présente</td><td>Commentaire</td></tr>
<tr><td>esi4-qcStatement-4</td><td>Cond.</td><td>Indique 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></td><td></td><td></td><td>esi4-qcStatement-6</td><td>Oui</td><td>Valeur « id-etsi-qct-eseal »

Indication que le certificat est un certificat qualifié de signature électronique</td></tr>
</table>

4) Compléments relatifs aux certificats qualifiés d'authentification de site internet

<table>
<tr><th>Field</th><th colspan="2">Value</th></tr>
<tr><td rowspan="4">Subject</td><td>Attribute</td><td>Value</td></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>
</table>

	organizationIdentifier	*(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 la norme européenne ETSI [EN_319_412-1] clause 5.1.4 À Monaco, ce numéro d'immatriculation peut également être constitué du préfixe « SI:MC- » suivi du numéro RCI
	commonName	*(Optionnel)* L'un des noms de domaine présents dans l'extension SubjectAltname
	Si le certificat a été délivré à une personne physique identifiée par son état civil	
	Attribute	**Value**
	givenName	Prénom usuel ou les prénoms de l'état civil du demandeur
	surname	Nom de l'état civil ou le nom d'usage du demandeur
	serialNumber	*(Optionnel)* Élément complémentaire permettant de distinguer les homonymes
	Si le certificat a été délivré à une personne physique identifiée par un pseudonyme	
	Attribute	**Value**
	Pseudonym	Pseudonyme du demandeur
	surname	Nom de l'état civil ou le nom d'usage du demandeur
	serialNumber	*(Optionnel)* Élément complémentaire permettant de distinguer les homonymes

Extension	Obligatoire	Critique	Valeur
Key Usage	Oui	Oui	Usages de clé conformes au chapitre 2.3.9 du présent document : digitalSignature et/ou keyEncipherment, ou keyAgreement
Subject Alternative Name	Oui	Non	Un ou plusieurs noms de domaine contrôlés par le responsable du certificat

<table>
<tr><td rowspan="4">QCStatements</td><td rowspan="4">Oui</td><td rowspan="4">Non</td><td colspan="3">Cette extension doit être conforme à la norme européenne ETSI [EN_319_ 412-5]</td></tr>
<tr><td>Extension</td><td>Présente</td><td>Commentaire</td></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>Valeur « id-etsi-qct-web » Indication que le certificat est un certificat qualifié de signature électronique</td></tr>
</table>

imprimé sur papier PEFC

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