

**SERVICES DE CRÉATION DE CERTIFICATS
QUALIFIÉS DE SIGNATURE ÉLECTRONIQUE, DE
CACHET ÉLECTRONIQUE ET D'AUTHENTIFICATION
DE SITE INTERNET**

**Annexe à l'arrêté ministériel n° 2020-894
du 18 décembre 2020**

**ANNEXE AU « JOURNAL DE MONACO » N° 8.519
DU 1^{ER} JANVIER 2021**

SOMMAIRE

1. Introduction.....	2
1.1. Objet.....	2
1.2. Cadre juridique.....	2
1.3. Mise à jour	3
1.4. Acronymes	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 des services de délivrance des certificats qualifiés	3
2.3. Compléments à la norme [EN_319_411-2]	4
2.3.1. Compléments relatifs à la vérification de l'identité du demandeur	4
2.3.2. Compléments relatifs à la constitution et la conservation du dossier de demande	5
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	6
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.....	7

Appendice 1 : Références documentaires.....	7
--	----------

Appendice 2 : Profils de certificats recommandés.....	8
--	----------

1) Socle commun à tous les profils de certificats	8
2) Compléments relatifs aux certificats qualifiés de signature électronique	10
3) Compléments relatifs aux certificats qualifiés de cachet électronique	11
4) Compléments relatifs aux certificats qualifiés d'authentification de site internet	12

1. Introduction

1.1. Objet

Dans le cadre du Référentiel Général de Sécurité de la Principauté, l'AMSN, désignée comme organe de contrôle, 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 annexe décrit les critères d'évaluation de la conformité aux exigences du Référentiel Général de Sécurité de la Principauté 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'arrêté ministériel n° 2020-893 du 18 décembre 2020 portant application de l'article 12 de l'Arrêté Ministériel n° 2020-461 du 6 juillet 2020, applicables à l'ensemble des prestataires de services de confiance qualifiés.

1.2. 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 paragraphe 2 du présent document sont présumés satisfaire aux exigences, respectivement, de l'annexe II, de l'annexe IV et de l'annexe V du Référentiel Général de Sécurité de la Principauté.

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 1163-3 du code civil.

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 1163-4 du code civil.

1.3. Mise à jour

Les mises à jour, les modalités de transition et date d'effet sont précisées par arrêté ministériel.

1.4. Acronymes

Les acronymes utilisés dans le présent document sont les suivants :

AMSN	Agence Monégasque de Sécurité Numérique
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
PSCE	Prestataires de Services de Certification Electronique
RGSP	Référentiel général de Sécurité de la Principauté
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

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'arrêté ministériel n° 2020-893 du 18 décembre 2020 portant application de l'article 12 de l'Arrêté Ministériel n° 2020-461 du 6 juillet 2020.

2.1.2. Inscription à 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*).

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 des services de délivrance des certificats qualifiés

L'évaluation doit permettre de démontrer le respect des exigences du RGSP 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 :

- Article 13, pour les prestataires de services de confiance qualifiés délivrant des certificats qualifiés, notamment les alinéas concernant :
 - La vérification de l'identité et des attributs spécifiques de la personne physique ou morale ;
 - L'utilisation de systèmes et des produits fiables, sécurité et fiabilité des processus ;
 - La conservation des informations délivrées et reçues dans le cadre de la délivrance des certificats qualifiés ;
 - La continuité de service suite à l'arrêt d'activité de délivrance de certificats qualifiés ;
 - La base de données relative aux certificats émis ;
 - La révocation des certificats ;
 - L'accès fiable, gratuit et efficace au statut de révocation des certificats.

- Article 20, 29 et 34, pour les certificats qualifiés.

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

2.3. Compléments à la norme [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 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.

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 ci-dessous 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 par une source disponible publiquement ; et
- que ce document ne paraît pas contrefait et ne présente pas de signe de falsification¹.

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. Compléments à la norme [EN_319_411-2]

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 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.

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.

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 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 2.3.1.1 et 2.3.1.2 ci-dessus.

Le PSCE doit mettre en œuvre un processus de validation de la signature ou du cachet répondant aux exigences prévues par le premier alinéa de l'article 24, du RGSP (à l'exception du 6^{ème} tiret concernant l'utilisation de dispositif de création de signature électronique qualifié), appliquées aussi 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.

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 la Principauté 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'AMSN.

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 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 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 [EN_319_411-2] ;
- pour une personne morale, toute pièce, valide lors de la demande de certificat, attestant de son existence et portant le numéro RCI de celle-ci, ou, à défaut, une autre pièce attestant l'identification unique de la personne morale qui figurera dans le certificat ;
- pour une personne morale, 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.

2.3.3. 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 l'arrêté ministériel n° 2020-893 du 18 décembre 2020 portant application de l'article 12 de l'Arrêté Ministériel n° 2020-461 du 6 juillet 2020.

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 en 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].

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 ; 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 2) ci-dessus 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 cryptopériode 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].
Cachet électronique (Personne morale)	
	La durée maximale de validité est de 3 ans.
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

Renvoi	Document
[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.
[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.
[RGSP]	Référéntiel Général de Sécurité de la Principauté : l'arrêté ministériel n° 2020-461 du 6 juillet 2020 portant application de l'article 13 de l'Ordonnance Souveraine n° 8.099 du 16 juin 2020 fixant les conditions d'application de la loi n° 1.383 du 2 août 2011 pour une Principauté numérique, modifiée, relative aux services de confiance.
[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

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 II, IV et V du RGSP.

Les certificats peuvent contenir d'autres champs ou extensions que ceux définis ci-dessous, en conformité avec la [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	Attribut	Valeur
	countryName	Nom du pays de l'autorité compétente auprès de laquelle le prestataire est officiellement enregistré (<i>tribunal de commerce, ministère, ...</i>)
	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 « NTRMC- » 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 paragraphes 2.3.7 et 2.3.8.	
Not After	Date de fin de validité du certificat, conformément aux règles des paragraphes 2.3.7 et 2.3.8.	
Subject	<i>Voir les règles applicables à chaque type de certificat, dans l'appendice 2 paragraphes 2), 3) et 4) de la présente annexe.</i>	
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 ambiguë du nom officiel du prestataire peut également être utilisée (par exemple, une abréviation reconnue et largement utilisée du nom officiel).

Extension	Obligatoire	Critique	Valeur		
Basic Constraints	Oui	Non	« CA:false ».		
Certificate Policies	Oui	Non	Identifiant de la Politique de Certification applicable.		
CRL Distribution Points	Conditionnel	Non	<p>Point de publication des listes de certificats révoqués.</p> <p>En cas d'absence d'un service OCSP :</p> <ul style="list-style-type: none"> • <i>un point de distribution des LCR est requis ;</i> • <i>le point de publication des LCR doit faire référence à une LCR publiée.</i> <p>Au moins une des LCR publiées doit être accessible selon le protocole http ou LDAP.</p>		
Authority Information Access	Oui	Non	<p>Renseignement de l'extension «<i>Authority Information Access</i>» :</p> <ul style="list-style-type: none"> • <i>accessMethod OID</i> valorisé à « <i>id-ad-caIssuers</i> » ; • <i>accessLocation</i> valorisé avec le chemin d'accès au certificat de l'AC (URL http de téléchargement du certificat de l'AC). <p>En complément, si un répondeur OCSP est mis en œuvre :</p> <ul style="list-style-type: none"> • <i>accessMethod OID</i> valorisé à « <i>id-ad-ocsp</i> » ; • <i>accessLocation</i> valorisé avec le chemin d'accès au répondeur OCSP (<i>obligatoire si aucune LCR n'est publiée</i>). 		
Key Usage	Oui	Oui	Voir les règles applicables à chaque type de certificat, dans les appendices 2 paragraphes 2), 3) et 4) de la présente annexe.		
qcStatements	Oui	Non	Extension	Présente	Commentaire
			Esi4-qcStatement-1	Oui	Indication de certificat émis est qualifié, via la valeur « <i>id-etsi-qcs-QcCompliance</i> »
			Esi4-qcStatement-2	Opt.	Extension optionnelle, décrite dans la norme [EN_319_412-5]
			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'appendice 2 paragraphes 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'appendice 2 paragraphes 2), 3) et 4).
Subject Alternative Name	Conditionnel	Non	Voir les règles applicables à chaque type de certificat, dans les appendices 2 paragraphes 2), 3) et 4) de la présente annexe.		
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	<i>(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</i>								
	organizationIdentifier	<i>(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</i> À Monaco, ce numéro d'immatriculation peut également être constitué du préfixe « NTRMC » suivi du numéro RCI								
	serialNumber	<i>(Optionnel) Élément complémentaire permettant de distinguer les homonymes</i>								
En cas d'utilisation de l'état civil du porteur :										
<table border="1"> <thead> <tr> <th>Attribute</th> <th>Value</th> </tr> </thead> <tbody> <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> </tbody> </table>			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.
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										
<table border="1"> <thead> <tr> <th>Attribute</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Pseudonym</td> <td>pseudonyme du porteur</td> </tr> <tr> <td>commonName</td> <td>pseudonyme du porteur</td> </tr> </tbody> </table>			Attribute	Value	Pseudonym	pseudonyme du porteur	commonName	pseudonyme du porteur		
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 : <i>nonRepudiation</i>		
Subject Alternative Name	Non	Non	<i>Cette extension ne devrait pas être présente.</i>		
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 (<i>tribunal de commerce, ministère, ...</i>).
	organizationIdentifier	Numéro d'immatriculation officiel de l'entité responsable du certificat conformément à [EN_319_412- 1] clause 5.1.4 A Monaco, ce numéro d'immatriculation peut également être constitué du préfixe « NTRMC- » 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.	

Extension	Obligatoire	Critique	Valeur		
Key Usage	Oui	Oui	Usages de clé conformes au paragraphe 2.3.9 du présent document : <i>digitalSignature</i> et/ou <i>nonRepudiation</i>		
Subject Alternative Name	Non	Non	<i>Cette extension ne devrait pas être présente.</i>		
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-eseal ». Indication que le certificat est un certificat qualifié de signature électronique.

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

Field	Value	
Subject	Attribute	Value
	countryName	Pays dans lequel est établi ou réside le demandeur
	localityName	Ville dans laquelle est établi ou réside le demandeur
	organizationName	<i>(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</i>
	organizationIdentifier	<i>(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</i> À Monaco, ce numéro d'immatriculation peut également être constitué du préfixe « NTRMC- » suivi du numéro RCI
	commonName	<i>(Optionnel) L'un des noms de domaine présents dans l'extension SubjectAltname</i>
	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	<i>(Optionnel) Elément complémentaire permettant de distinguer les homonymes</i>
	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	<i>(Optionnel) Elément complémentaire permettant de distinguer les homonymes</i>	

Extension	Obligatoire	Critique	Valeur		
Key Usage	Oui	Oui	Usages de clé conformes au paragraphe 2.3.9 : <i>digitalSignature</i> et/ou <i>keyEncipherment</i> , ou <i>keyAgreement</i>		
Subject Alternative Name	Oui	Non	Un ou plusieurs noms de domaine contrôlés par le responsable du certificat		
QCStatements	Oui	Non	Cette extension doit être conforme à [EN_319_412-5]		
			Extension	Présente	Commentaire
			esi4- qcStatement-4	Non	<i>Cette extension ne devrait pas être présente</i>
esi4- qcStatement-6	Oui	Valeur « id-etsi-qct-web ». Indication que le certificat est un certificat qualifié de signature électronique.			

