ROYAUME DU MAROC
ADMINISTRATION DE LA DEFENSE NATIONALE
DIRECTION GENERALE DE LA SECURITE
DES SYSTEMES D'INFORMATION

Référentiels d'exigences relatifs aux services de confiance qualifiés et aux prestataires fournissant ces services

2

[Ref_Deliv_Cert_Qual]

Exigences de conformité des prestataires fournissant des services de **délivrance de certificats électroniques qualifiés**

(Pour signature électronique ou cachet électronique
ou authentification de site internet)

Suivi des mises à jour du document [Ref_Deliv_Cert_Qual]

Date	Version	Rédacteur	Détail évolution
13/07/2023	1.0	DGSSI	Version initiale

Pour toute question ou information concernant ce document, s'adresser à :

PSCo-dsr@dgssi.gov.ma

Sommaire

1 Terminologie et acronymes

AC : Autorité de certification.

Autorité nationale : fait référence à l'autorité nationale des services de confiance pour les transactions électroniques au sens du décret n° 2.22.687 ; à savoir la Direction Générale de la Sécurité des Systèmes d'Information (DGSSI).

CRL : Certificate revocation List (en français LCR : Liste des certificats révoqués).

DeltaLCR : Mécanisme par lequel la CRL se met à jour via des incrémentations.

DPC : Déclaration des Pratiques de Certification.

http : hypertext transfer protocol.

LDAP : Lightweight Directory Access Protocol.

Liste nationale des PSCo agréés (LNPA) par l'autorité nationale : désigne, conformément à l'article 53 de la Loi 43-20, la liste publiée par l'autorité nationale sur son site internet et qui consolide l'ensemble des prestataires de services de confiance agréés par l'autorité et les services de confiance qualifiés qu'ils fournissent.

OCSP : Online Certificate Status Protocol est un protocole internet permettant d'accéder au statut d'un certificat et de vérifier sa validité en temps réel.

PC : Politique de Certification.

PKI : Public Key Infrastructure.

PSCo : prestataire de service de confiance au sens de la Loi n° 43-20.

PSCo agréé : désigne un prestataire de service de confiance agréé par l'autorité nationale qui fournit un ou plusieurs services de confiance qualifiés conformément à la Loi n° 43-20.

QSCD : *(Qualified Signature/Seal Creation Device)* Dispositif de création de signature/cachet électroniques qualifiés au sens de la loi 43-20 et conformément à la norme 319 411-2.

QCP-l : *(Qualified Certificate Policy issued to a legal person)* Politique de certificat qualifié pour une personne morale au sens de la loi 43-20 et conformément à la norme 319 411-2.

QCP-n : *(Qualified Certificate Policy issued to a natural person)* Politique de certificat qualifié pour une personne physique au sens de la loi 43-20 et conformément à la norme 319 411-2.

QCP-n-QSCD : (Policy for Qualified Certificate issued to a natural person where the private key and the related certificate reside on a QSCD) Politique pour certificat qualifié délivré à une personne physique pour lesquels la clé privée et le certificat associé sont contenus au niveau d'un dispositif de création de signature/cachet électroniques qualifiés (conformément à la norme 319 411-2).

URL : Uniform Resource Locator.

UTC : Temps Universel Coordonné (Coordinated Universal Time).

Profil de protection : document public qui définit, pour une catégorie de produits, un ensemble d'exigences et d'objectifs de sécurité, indépendants de leur technologie et de leur implémentation, qui satisfont les besoins de sécurité communs à un groupe d'utilisateurs.

2 Objet et périmètre

Le présent document, désigné par **[Ref_Deliv_Cert_Qual]**, constitue le référentiel fixant les exigences de conformité à respecter par les PSCo agréés fournissant des **services de délivrance de certificat qualifiés** et ce conformément au **cadre légal national** rappelé dans le présent document notamment au niveau du chapitre « Cadre de référence ».

Le respect des exigences des référentiels [Ref_Deliv_Cert_Qual] & [Ref_PSCo_AG] conditionnent l'obtention de l'agréement pour la fourniture des services de délivrance de certificats qualifiés.

L'évaluation du respect des exigences est assurée par l'autorité nationale conformément aux dispositions décrites au niveau de la Loi 43-20 et ses textes d'application (article 54 Loi 43-20).

Les PSCo fournissant des services de confiance additionnels, devront se conformer aux référentiels applicables selon la nature du service fourni.

3 Modalités de mise à jour

L'autorité nationale veille à ce que le référentiel d'exigences reste en cohérence avec le cadre réglementaire nationale et aligné avec les bonnes pratiques.

Dans ce sens, le présent document peut faire l'objet de mise à jour ou d'ajustements ultérieurs.

En cas de mise à jour ou d'ajustement, l'autorité l'indique sur son site internet et précise la date d'effet ainsi que les éventuelles dispositions transitoires applicables.

4 Cadre de référence

4.1 Cadre juridique et normatif

Le cadre légal de référence sur lequel repose **[Ref_Deliv_Cert_Qual]** est comme suit :

- Les dispositions de la **loi n° 43-20** relative aux services de confiance pour les transactions électroniques promulguée par le dahir n° 1-20-100 du 16 joumada I 1442 (31 décembre 2020)
    - Les principales dispositions spécifiques de la loi n°43-20 sont rappelées au niveau du chapitre 4.3 du présent document ;
- Les dispositions du **décret n° 2.22.687** pris pour l'application de la loi n°43-20 :
    - Les principales dispositions spécifiques du décret n° 2.22.687 sont rappelées au niveau du chapitre 4.4 du présent document.

En addition, **[Ref_Deliv_Cert_Qual]** explicite, quand cela est nécessaire, les modalités organisationnelles et techniques pour la mise en œuvre des dispositions précitées, en s'appuyant sur des normes, des standards et des compléments :

- **[Norme] ETSI EN_319_411-2** v2.4.1 (2021-11) ou version ultérieure **:** 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.

  Définit les exigences normatives relatives aux prestataires de services de confiance fournissant un service de délivrance de certificats qualifiés ;

  Elle fait appel notamment à la **[Norme] ETSI EN_319_411-1:** Electronic Signatures and Infrastructures (ESI) ; Policy and security requirements for Trust Service Providers issuing certificates ; Part 1: General requirements.

  Définit les exigences générales relatives aux services de délivrance de certificats électroniques ;

- **[Standard] ETSI TS 119 461** V1.1.1 (2021-07) ou version ultérieure **:** Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects.

  Définit les exigences normatives relatives à la vérification de l'identité dans le cadre du processus d'enrôlement d'un utilisateur souhaitant bénéficier d'un service de confiance numérique (typiquement, la vérification de l'identité au vu de la délivrance d'un certificat électroniques qualifié) ;

- **[Normes] ETSI EN 319 412-1/2/3/4/5,** Electronic Signatures and Infrastructures (ESI) ; Certificate Profiles.

  Définit les exigences normatives relatives aux profils des certificats ;

- **[Compléments]** Ensemble d'exigences ou de spécifications additionnelles, en complément des normes ou des articles de la loi/décret, qui ont pour objectifs de compléter ou de préciser les modalités de mise en œuvre de points spécifiques.

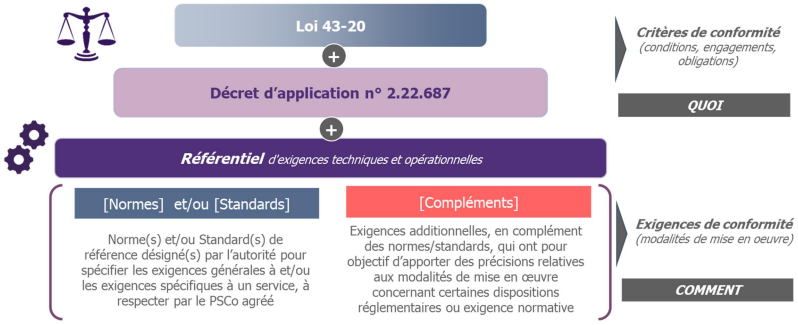


Figure 1 : Structure du cadre juridique et normatif

4.2 Précaution d'interprétation des normes et standards ETSI

Les normes et standards ETSI, CEN et ISO sur lesquels s'appuie l'autorité nationale, pour l'élaboration des référentiels d'exigences relatifs aux services de confiance et aux PSCo, représentent un cadre de référence solide, mature, largement adopté et unanimement reconnu à l'international.

L'utilisation de ce cadre présente un double avantage :

- Garantir la fiabilité, la sécurité, la pérennité et la robustesse des services de confiance délivrés au niveau national ;
- Permettre la reconnaissance à l'international des services délivrés par les PSCo établis au niveau national et faciliter les échanges électroniques avec les pays partenaires.

L'ensemble des exigences et recommandations de ces Normes reprises dans les référentiels ont été rédigés de sorte qu'elles soient généralement applicables indépendamment du contexte. Ils contiennent cependant certaines références, peu impactantes, au contexte normatif Européen très proche du contexte normatif national.

Afin d'éviter toute ambiguïté et garantir la transposition des normes ETSI et CEN au contexte national**,** les PSCo sont tenus de prendre en compte les instructions et précautions de lecture suivantes **:**

- Les références au cadre réglementaire Européen « Directive 95/46/EC » ou « Regulation (EU) No 910/2014 » et aux chapitres et articles associés, doivent être replacées et interprétées dans le contexte national :
  - Le cadre réglementaire à prendre en compte est bien le cadre national à savoir la **« Loi 43-20 »** et son **« Décret d'application n° 2.22.687 »** tel que rappelé dans ce document ;
  - Les dispositions, articles et chapitres concernant la prestation ou le service de confiance objet du référentiel sont rappelés dans le corps de chaque référentiel ;
- Le terme **« EU qualified »** est à transposer en **:**
  - **« Agréé »** lorsqu'il s'agit d'un **PSCo ;**
  - **« Qualifié »** lorsqu'il s'agit d'un **service de confiance ;**
- Les « **EU official languages** » (langues officielles européennes) à considérer dans le contexte national sont **l'anglais** et/ou le **français** ;
- Comme précisé par l'ETSI, les termes « s**hall / shall not** » indiquent des **exigences obligatoires** qui doivent être **strictement respectées** et **mises en œuvre** par le PSCo :
  - Plus largement, les verbes modaux et auxiliaires utilisés dans les différentes normes ETSI sont à interpréter conformément aux indications de la clause 3.2 de **l'ETSI Drafting Rules ;**
- En cas de doute concernant une référence très spécifique à l'Union Européenne, jugée non applicable dans le contexte national par le PSCo ➔ se rapprocher de l'autorité nationale.

4.3 Rappel des principales dispositions de la loi n°43-20 applicables

En sus des dispositions générales applicables à l'ensemble des PSCo, les principaux articles et dispositions de la loi n° 43-20 applicables spécifiquement aux PSCo agréés fournissant des services de délivrance de certificats qualifiés de signatures/cachets électroniques et d'authentification de sites internet, sont consolidés au niveau du tableau suivant :

Chapitre Ier **Section Ière** *Des service de confiance*	**Article 6**	Une signature électronique qualifiée est produite par un dispositif qualifié de création de signature et repose sur un **certificat électronique qualifié** de signature électronique.
	Article 9	Les données et informations contenues dans le certificat qualifié de signature électronique sont fixées par voie réglementaire.
	Article 18	Les données et informations contenues dans le certificat qualifié de cachet électronique sont fixées par voie réglementaire.
	Article 31	Les données et informations contenues dans le certificat qualifié d'authentification du site internet sont fixées par voie réglementaire.
Chapitre Ier **Section II** Des prestataires de service de confiance	**Article 32**	Obligation d'agréement : seuls les prestataires de services de confiance agréés peuvent fournir un service* de confiance qualifié et gérer les opérations y afférentes. * ici le service de délivrance de certificat qualifié.
	Article 33	Utilisation, dans le cadre de la délivrance de certificat, de systèmes, matériels et logiciels fiables ; et garantie de leur sécurité technique et de la fiabilité des processus pris en charge. Modalités de vérification de l'identité et des attributs spécifiques de la personne physique ou morale + Possibilité de délégation de la vérification de l'identité + Révocation du certificat + Informations relatives au statut du certificat.
	Article 39	Obligation pour le PSCo de conserver les données relatives à la fourniture du service* de confiance. Le cas échéant obligation de les communiquer aux autorités judiciaires en informant la partie utilisatrice. * ici le service de délivrance de certificat qualifié.
	Article 40	Obligation de notification en cas d'atteinte à la sécurité ou perte d'intégrité relative à un service* ou à des données à caractères personnelle. * ici le service de délivrance de certificat qualifié.
Chapitre Ier **Section III** Des obligations du titulaire de certificat électronique	**Article 41**	Responsabilité du titulaire du certificat électronique quant aux données afférentes à la création de la signature/cachet électronique qualifié lorsqu'elles se trouve dans son QSCD.
	Article 42	Obligation pour le titulaire du certificat de notifier, au plus tôt, le PSCo de toute modification des informations contenues dans ce certificat électronique.
	Article 43	Obligation pour le titulaire du certificat de faire révoquer ce dernier immédiatement en cas de doute sur : - la perte de la confidentialité relative aux données afférentes à la création de la signature/cachet électronique ; - ou la perte de conformité à la réalité pour les informations contenues dans le certificat.
	Article 44	Obligation pour le titulaire d'un certificat électronique de ne plus l'utiliser dès lors que ce dernier (le certificat) arrive à échéance ou qu'il a été révoqué.

Tableau 1: *Récapitulatif des principaux articles et dispositions de la loi 43-20 relatifs au service de délivrance de certificats qualifiés*

4.4 Rappel des principales dispositions du décret n° 2.22.687 applicables

En sus des dispositions générales applicables à l'ensemble des PSCo, les principaux articles et dispositions du décret n° 2.22.687 applicables spécifiquement aux PSCo agréés fournissant des services de délivrance de certificats qualifiés de signatures/cachets électroniques et d'authentification de sites internet, sont consolidés au niveau du tableau suivant :

Chapitre Ier **Section Ière** Des services de confiance qualifiés	**Article 2**	Informations (attributs) contenues dans le certificat qualifié de **signature électronique** délivré par le PSCo des services de confiance agréé.
	Article 3	Informations (attributs) contenues dans le certificat qualifié de **cachet électronique** délivré par le prestataire des services de confiance agréé
	Article 4	Informations (attributs) contenues dans le certificat qualifié **d'authentification d'un site internet** délivré par le prestataire des services de confiance agréé.
Chapitre II **Section Ière** Des prestataires de services de confiance agréés	**Article 13**	Constituants du dossier d'agrément (Annexe 2) relatifs au service* de confiance qualifié objet de la demande. Obligation de notification en cas de modification durant la période d'examen. * ici service de délivrance de certificat qualifié.
	Article 18	Obligation pour le PSCo de conserver des données relatives à la fourniture des services* de confiance qualifiés sur une période de 7 ans + Renvoi vers les référentiels d'exigences pour spécifier les types des données à conserver. * ici service de délivrance de certificat qualifié.
	Article 20	Reconnaissance de la CNIE comme moyen d'identification électronique qui aide à vérifier à distance l'identité en vue de la délivrance d'un certificat qualifié . +Ouverture à tout autre document électronique qui permet, conformément au texte législatif ou réglementaire qui l'institue, de prouver l'ID à distance de son titulaire et qui répond aux spécifications techniques minimales fixées par l'autorité.

Tableau 2 : *Récapitulatif des principaux articles et dispositions du décret n° 2.22.687 relatifs au service de délivrance de certificats qualifiés*

4.5 Interprétation du contenu des certificats

Afin de permettre une meilleure lecture du décret, ci-après un tableau de correspondance entre :

/ Les informations indiquées au niveau des articles 2, 3 et 4 du décret n°2.22.687 (attributs / contenu minimum des certificats) ;

Et

/ Les champs des profils type des certificats conformément à la [RFC 5280] explicités plus en détail plus bas dans le document avec les normes en vigueur au niveau de la section « exigences de conformité ».

Contenu minimum des certificats (articles 2/3/4 du décret 2.22.687)	
Information indiquée au niveau du décret	**Champ correspondant**
Code d'identité du certificat qualifié, qui doit être unique pour le prestataire de services de confiance agréé.	**Serial Number**
Identité et adresse du prestataire de services de confiance agréé.	**Champ Issuer**
Indication du début et de la fin de la durée de validité du certificat qualifié.	**Champs Validité** (Not Before et Not After)
Nom du signataire ou un pseudonyme le cas échéant. Si un pseudonyme est utilisé, cela doit être clairement indiqué.	**Champ Subject**
Données afférentes à la vérification de signature électronique qui correspondent aux données de création de la signature électronique.	**Clé publique**
Emplacement des services qui peuvent être utilisés pour s'informer du statut de validité du certificat qualifié. Endroit où peut être obtenu gratuitement le certificat sur lequel reposent la signature électronique avancée ou le cachet électronique avancé mentionnés au point.	**Point publication CRL** et **Accès OCSP**
Mention indiquant, au moins sous une forme adaptée au traitement automatisé, que le certificat a été délivré comme certificat qualifié de signature* électronique. Lorsque les données de création de la signature* électronique associées aux données de validation de la signature électronique se trouvent dans un dispositif qualifié de création de signature électronique, une mention l'indiquant, au moins sous une forme adaptée au traitement automatisé.	**Champ Key Usage** *(ici – signature* électronique*) et **QCStatements** *(certificat qualifié et dispositif qualifié)*
** (remplacer signature par cachet ou authentification web pour les articles 3 & 4)*	
Signature électronique avancée ou le cachet électronique avancé du prestataire de services de confiance agréé délivrant le certificat qualifié.	**Signature de l'AC**

Tableau 3 : *Informations contenues dans les certificats – correspondance décret vs. RFC 5280*

5 Procédure d'agrément

Pour un PSCo souhaitant délivrer des certificats qualifiés de signature électronique et/ou de cachet électronique et/ou d'authentification de site internet.

5.1 Modalités

Le processus d'agrément d'un PSCo, pour la fourniture du service de délivrance de certificats qualifiés de signature électronique, de cachet électronique et d'authentification de site internet, est décrit au niveau du référentiel **[Ref_PSCo_AG].**

Les critères de conformité et les exigences associées conditionnant l'obtention de l'agrément pour la délivrance de certificats qualifiés, sont précisés plus bas dans le présent document. Ils sont à compléter, de façon cumulative, par les exigences de conformité du référentiel **[Ref_PSCo_AG].**

5.2 Critères de conformité

En vue de l'obtention de l'agrément lui permettant la fourniture de certificats qualifiés, le PSCo est tenu de respecter l'ensemble des **conditions et des engagements** (désignés ci-après par **Critères**), prévus par les dispositions de la loi n° 43-20 et du décret n° 2.22.687, à savoir :

(Critère 1) Être agréé **:** seul un PSCo agréé au titre de la Loi 43-20 et ses textes d'applications, peut émettre et délivrer un certificat électronique qualifié et gérer les opérations y afférentes (article 32 de la loi n°43-20) ;

(Critère 2) Utiliser des systèmes, matériels et logiciels fiables et assurer leur sécurité technique (article 33 de la loi n°43-20) ;

(Critère 3) Assurer la fiabilité des processus mis en œuvre (article 33 de la loi n°43-20) ;

(Critère 4) Préciser de façon exhaustive les conditions et limites d'utilisation des services de confiance (ici service de délivrance de certificats qualifiés) avant l'établissement d'une relation contractuelle avec un futur client/utilisateur (article 33.2.a de loi n°43-20) ;

(Critère 5) Garantir la conservation pendant sept (7) ans, de manière sécurisée avec accès contrôlé et limité (publication soumise à consentement de l'intéressé), des données pertinentes concernant les échanges relatifs à la fourniture des services de confiance (ici service de délivrance de certificats qualifiés).
(articles 33.2.b et 39 de la loi n°43-20, article 18 du décret 2.22.687) ;

(Critère 6) Assurer la vérification de l'identité (ou de tout autre information) de la personne morale ou physique à qui le certificat est délivré (article 33 de la loi n°43-20) ;

(Critère 7) Garantir que les certificats qualifiés de signatures électroniques comportent a minima les informations précisées au niveau de l'article 2 du décret d'application n° 2.22.687 (article 9 de la loi n°43-20 et article 2 du décret d'application n° 2.22.687) ;

(Critère 8) Garantir que les certificats qualifiés de cachet électronique comportent a minima les informations précisées au niveau de l'article 3 du décret d'application n° 2.22.687 (article 18 de la loi n°43-20 et article 3 du décret d'application n° 2.22.687) ;

(Critère 9) Garantir que les certificats qualifiés d'authentification d'un site internet comportent a minima les informations précisées au niveau de l'article 4 du décret d'application n° 2.22.687 (article 31 de la loi n°43-20 et article 4 du décret d'application n° 2.22.687) ;

(Critère 10) Permettre à la personne à qui le certificat a été délivré de révoquer sans délai et avec certitude son certificat (article 33 de la loi n°43-20) ;

(Critère 11) Garantir que la date et l'heure de délivrance et de révocation du certificat électronique peuvent être déterminées avec précision et publier le statut du certificat dès sa révocation et maintenir ces informations disponibles à tout moment et au-delà de la période de validité des certificats (article 33 de la loi n°43-20) ;

(Critère 12) S'assurer que le titulaire du certificat électronique est bien informé de la nécessité de notifier le prestataire de confiance de confiance au sujet de toute modification des informations contenues dans ce certificat (article 42 de la loi n°43-20) ;

(Critère 13) Mise en place des moyens et procédures permettant, en cas d'arrêt des activités du PSCo :

- De garantir la reprise de ses activités par un prestataire de services de confiance assurant un niveau équivalent de qualité et de sécurité ;
- Ou à défaut, de révoquer les certificats électroniques dans un délai maximum de deux mois après en avoir averti les titulaires.

(Article 37 de la loi n°43-20).

A noter :

Le respect de ces critères de conformité se matérialise par la **mise en œuvre,** de la part du PSCo souhaitant fournir un service de **délivrance de certificats qualifiés,** des dispositions ci-dessous :

- **Exigences de conformité** spécifiées dans [**Ref_PSCo_AG**] applicables à l'ensemble des PSCo souhaitant fournir un **service de confiance qualifié ;**
- **Exigences de conformité,** spécifiques au PSCo souhaitant fournir des **certificats qualifiés,** listées **dans le présent document** (chapitre « Exigences de conformité »).

6 Exigences de conformité

Ref_Deliv_Cert_Qual_Exig 1. Le PSCo souhaitant fournir des services de délivrance de certificats qualifiés est tenu de prendre connaissance de l'ensemble des documents constituants le cadre juridique et normatif. Il est entendu que les différents textes normatifs s'expliquent mutuellement. Cependant, en cas d'incohérence entre d'une part une spécification dans l'une des normes et d'autre part une disposition précise de la loi 43-20 ou de son décret d'application, ces derniers (loi et/ou décret) prévaudront. Dans ce cas, le PSCo remonte la suspicion d'incohérence à l'autorité nationale, avant implémentation, afin de clarifier le point et le cas échéant procéder éventuellement à une rectification.

Ref_Deliv_Cert_Qual_Exig 2. Le PSCo souhaitant fournir des services de délivrance de certificats qualifiés (de signature électronique, de cachet électronique ou d'authentification de site internet) doit être agréé au sens de la loi 43-20 et son décret d'application. A ce titre, le PSCo doit impérativement se conformer aux exigences du référentiel **[Ref_PSCo_AG].**

6.1 Normes applicables

6.1.1 Norme ETSI 319 411-2

Ref_Deliv_Cert_Qual_Exig 3. Les PSCo souhaitant fournir des certificats qualifiés (de signature électronique, de cachet électronique ou d'authentification de site internet) sont tenus de se conformer à l'ensemble des exigences de la norme **ETSI EN 319 411-2** v2.4.1 ou ultérieure. Cela comprend :

- Les exigences relatives aux dispositions générales sur la déclaration des pratiques et les politique de certificat (*chap. 5 – General provisions on Certification Practice Statement and Certificate Policies*) y inclut :
  - Exigences générales (5.1 General requirements) ;
  - Déclaration des pratiques de certification *(5.2 Certification Practice Statement requirements) ;*
  - Nomenclature et identification de la politique de certification *(5.3 Certificate Policy name and identification) ;*
  - Intervenants et acteurs de la PKI *(5.4 PKI participants) ;*
  - Usage du certificat *(5.5 Certificate usage) ;*
- Les exigences relatives aux pratiques des prestataires de services de confiance (*chap. 6 – Trust Service Providers practice*) y inclut :
  - *Responsabilités relatives à la publication et au dépôt (6.1 Publication and repository responsibilities) ;*
  - *Identification et authentification (6.2 Identification and authentication) ;*
  - *Exigences opérationnelles relatives aux cycles de vie des certificats (6.3 Certificate Life-Cycle operational requirements) ;*
  - *Installation, gestion et contrôle opérationnel (6.4 Facility, management and operational controls) ;*
  - *Contrôles Techniques de la sécurité (6.5 Technical security controls) ;*
  - *Profils des Certificat, CRL et OCSP (6.6 Certificate, CRL and OCSP profiles) ;*
  - *Audit de conformité et autres évaluations (6.7 Compliance audit and other assessment) ;*
  - *Autres questions commerciales et juridiques (6.8 Other business and legal matters) ;*

- *Autres dispositions (6.9 Other provisions);*

➢ Les exigences relatives au cadre de définition d'autres politiques de certificats (*chap. 7 – Framework for the definition of other certificate policies*) y inclut :

- *Gestion de la politique de certificat (7.1 Certificate policy management)*
- *Exigences complémentaires (7.2 Additional requirements)*

La norme ETSI 319 411-2 peut renvoyer vers d'autres normes ETSI ou vers l'ISO/IEC 27005 pour donner des orientations de mise en œuvre de certaines exigences.

Certaines exigences sont complétées et/ou précisées par des compléments spécifiés plus bas dans le document.

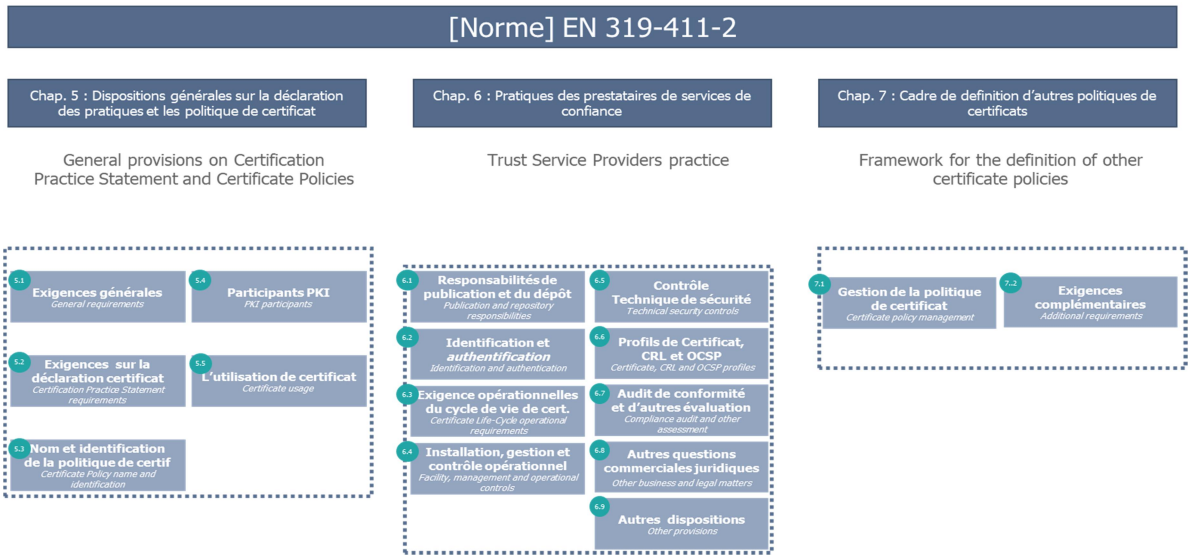


Figure 2 - Sujets couverts par la norme ETSI EN_319_411-2

6.1.2 Normes ETSI 319 412-1/2/3/4/5

Ref_Deliv_Cert_Qual_Exig 4. En fonction de la nature de l'usage du certificat qualifié qu'il souhaite fournir, le PSCo agréé respectera les exigences de la norme ETSI 319 412-1/2/3/4/5 comme suit :

Cas de certificat qualifié de signature électronique :

- Lorsque le PSCo entend délivrer des **certificats qualifiés de signature électronique**, le respect de la norme **ETSI EN 319 412-2 est obligatoire.** Cela comprend :
  - ➢ Les exigences générales du profil des Certificats *(Chap. 4 - General certificate profile requirements) :*
    - Exigences génériques *(4.1 Generic requirements) ;*
    - Champs de base du certificat *(4.2 Basic certificate fields) ;*
    - Extensions standard du certificat *(4.3 Standard certificate extensions) ;*
    - Extensions Internet IETF RFC 5280 du certificat *(4.4 IETF RFC 5280 internet certificate extensions) ;*
  - ➢ Les exigences relatives au certificat qualifié *(Chap. 5- Exigences relative au certificat qualifié de l'UE) :*
    - EU QCStatements *(5.1 EU QCStatements) ;*

- Politiques du certificat *(5.2 Certificate policies) ;*

Cas de certificat qualifié de cachet électronique :

- Lorsque le PSCo entend délivrer des **certificats qualifiés de cachet électronique**, le respect de la norme **ETSI EN 319 412-3 est obligatoire.** Cela comprend :
  - Les exigences relatives aux profils *(chap. 4 - Profiles requirements) :*
    - Les exigences génériques *(4.1 Generic requirements) ;*
    - Les champs de base des certificats *(4.2 Basic certificate fields) ;*
    - Les extensions standards des certificats *(4.3 Standard certificate extensions).*

Cas de certificat qualifié d'authentification de sites internet :

- Lorsque le PSCo entend délivrer des **certificats qualifiés d'authentification de sites internet**, le respect de la norme **ETSI EN 319 412-4** est obligatoire**.** Cela comprend :
  - Les exigences du profil *(Chap. 4 - Profile requirements) ;*
    - Exigences génériques du profile *(4.1 Generic profile requirements) ;*
    - QCStatements pour les certificats conformes QEVCP-w ou QNCP-w *(4.2 EU Qualified Certificate statements for Certificates following QEVCP-w or QNCP-w) ;*
    - Politiques de certification pour les certificats conformes à QEVCP-w ou QNCP-w *(4.3 Certificate policies for Certificates following QEVCP-w or QNCP-w).*

Tout certificat qualifié :

- Le respect de la norme ETSI EN 319 412-5 est obligatoire quelle que soit la nature de l'usage du certificat qualifié. Cela comprend :
  - Les exigences relatives à la déclaration de certificats qualifiés *(chap. 4 - Qualified certificate statements) ;*
  - Les exigences relatives à QCStatements au niveau des certificats qualifiés *(chap. 5 - Requirements on QC Statements in EU qualified certificates).*

6.2 Compléments et précisions

Les exigences de ce chapitre sont des compléments ou précisions en addition :

- Aux dispositions des normes applicables ETSI EN EN 319 411-2 et ETSI EN 319 412-1/2/3/4/5 ;
- Aux dispositions des articles applicables de la loi 43-20 et du décret 2.22.687.

6.2.1 Dossier d'enregistrement

Ref_Deliv_Cert_Qual_Exig 5. 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 notamment une copie de la carte nationale d'identité électronique en cours de validité du futur titulaire ou tout document valide justifiant son identité (comportant une photo d'identité et délivré par une autorité compétente) ;

- Les conditions générales d'utilisation (conformément à la norme [EN_319_411-2] notamment la clause 6.3.4), dans leur version en vigueur, signées par le demandeur ;
- Lorsque le futur titulaire du certificat est un mineur ou un incapable majeur, la demande de certificat et les conditions générales d'utilisation sont signées par son représentant (tuteur ou administration légale). Ce dernier joint également à la demande :
    - Une copie de sa propre carte nationale d'identité électronique en cours de validité ou tout document valide justifiant son identité (comportant une photo d'identité et délivré par une autorité compétente) ;
    - Un document justifiant son statut de représentant du mineur ou de l'incapable majeur ;
    - Une preuve de l'incapacité ou de l'âge du futur titulaire ;

Ref_Deliv_Cert_Qual_Exig 6. 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 norme [EN_319_411-2] notamment la clause 6.3.4) ;
- Pour une entreprise :
    - Toute pièce, valide lors de la demande de certificat, attestant de l'existence de l'entreprise et portant un numéro d'immatriculation officiel (numéro d'inscription au registre du commerce, numéro ICE…) de celle-ci, ou, à défaut, une autre pièce attestant l'identification unique de l'entreprise qui figurera dans le certificat ;
    - Et tout document attestant de la qualité du demandeur de certificat ;
- Pour une personne morale de droit public (administration, établissement public ...) :
    - Un document, valide au moment de l'enregistrement, portant délégation de l'autorité responsable de la structure administrative ou de l'établissement public.

Ref_Deliv_Cert_Qual_Exig 7. Lorsque la demande de certificat et/ou les conditions générales d'utilisation sont présentées sous format papier (demande manuscrite, demande imprimée, CGU imprimées…) elles doivent obligatoirement être signées de façon manuscrite par le demandeur (personne physique ou le représentant autorisé de la personne morale).

Ref_Deliv_Cert_Qual_Exig 8. Lorsque la demande de certificat et les conditions générales d'utilisation sont de nature électronique, elles peuvent être :

- Signées électroniquement au moyen d'une signature électronique avancée lorsqu'il s'agit d'un certificat qualifié de signature électronique ou d'authentification de site internet, sous la responsabilité d'une personne physique ;
- Signées (ou cachetées) électroniquement au moyen d'une signature électronique avancée (ou cachet électronique avancé) lorsqu'il s'agit d'un certificat qualifié de cachet électronique ou d'authentification de site internet, sous la responsabilité d'une personne morale.

6.2.2 Mandataire de certification

Ce chapitre ne concerne que la délivrance de certificat à une personne morale ou à une personne physique dans le cadre de son appartenance à une entité personne morale (désignée par entité cliente dans ce chapitre).

L'enregistrement d'un titulaire (personne physique ou morale) de certificat peut se faire soit directement auprès de l'autorité d'enregistrement, soit via un mandataire de certification de l'entité cliente dont il dépend.

Ref_Deliv_Cert_Qual_Exig 9. En cas de recours à un mandataire, celui-ci doit être formellement désigné par un représentant légal de l'entité concernée et doit être enregistré par l'autorité d'enregistrement.

Ref_Deliv_Cert_Qual_Exig 10. Le dossier d'enregistrement d'un mandataire doit au moins comprendre :

- Une copie de la carte nationale d'identité électronique en cours de validité du mandataire ou tout document valide justifiant son identité (comportant une photo d'identité et délivré par une autorité compétente) ;
- Un mandat daté de moins de 3 mois co-signé par un représentant légal de l'entité désignant le mandataire et par le par le mandataire pour acceptation ;
- Une attestation d'engagement datée de moins de 3 mois et signée par le mandataire, qui atteste de l'engament du mandataire auprès de l'AC à respecter ses obligations notamment :
    - Réaliser correctement et de façon intègre, fiable et indépendante les contrôles des dossiers de demande de certificat et les contrôles des identités des futurs titulaires ;
    - Signaler sans délai à l'autorité d'enregistrement son départ de l'entité ;
- Pour l'entité cliente :
    - [Entreprise] toute pièce, valide lors de la demande de certificat (extrait Kbis ...), attestant de l'existence de l'entreprise, portant sa raison sociale et un Numéro d'immatriculation officiel (ICE, numéro d'inscription au registre du commerce, …) ou, à défaut, une autre pièce attestant l'identification unique de l'entreprise qui figurera dans le certificat ;
    - [Administration] une pièce, valide au moment de l'enregistrement, portant délégation de l'autorité responsable au sein de la structure administrative.

Ref_Deliv_Cert_Qual_Exig 11. Les engagements du mandataire à l'égard de l'autorité de certification doivent être précisés dans un contrat écrit avec l'entité cliente du mandataire. Ce contrat stipule notamment que le mandataire doit :

- Respecter les parties de la PC et de la DPC de l'AC qui lui incombent ;
- Réaliser correctement et de façon intègre, fiable et indépendante les contrôles des dossiers de demande de certificats et les contrôles des identités des futurs titulaires (ou des représentants légaux si le titulaire est une personne morale) :
    - Il assure notamment le face-à-face pour l'identification des titulaires lorsque celui-ci est requis ;
- Signaler sans délai à l'autorité d'enregistrement son départ de l'entité.

Ref_Deliv_Cert_Qual_Exig 12. Le procédé de délivrance de certificat, décrit dans la PC, doit garantir que le mandataire ne peut avoir accès à des moyens qui lui permettraient d'activer et d'utiliser la clé privée associée à la clé publique contenue dans le certificat délivré au titulaire.

Ref_Deliv_Cert_Qual_Exig 13. Le dossier d'enregistrement d'un (futur) titulaire via un mandataire, doit au moins comprendre :

- Une demande de certificat, datée de moins de 3 mois, indiquant l'identité du titulaire, co-signé par le mandataire et le titulaire *(ou le représentant légal de l'entité titulaire dans le cas d'une personne morale) ;*
- Une copie de la carte nationale d'identité électronique en cours de validité du futur titulaire *(ou le représentant légal de l'entité titulaire dans le cas d'une personne morale)* ou tout

document valide justifiant son identité délivré (comportant une photo d'identité et délivré par une autorité compétente) ;

- Les conditions générales d'utilisation signées par le titulaire *(ou le représentant légal de l'entité titulaire dans le cas d'une personne morale) ;*
- L'adresse postale et / ou l'adresse mail permettant à l'autorité de certification de contacter le titulaire *(ou le représentant légal de l'entité titulaire dans le cas d'une personne morale).*

Ref_Deliv_Cert_Qual_Exig 14. La vérification de l'identité du mandataire est réalisée conformément aux dispositions spécifiées dans ce document, relatives à la vérification de l'identité au vu de la délivrance d'un certificat qualifié.

6.2.3 Personne autorisée

Il s'agit d'une personne physique autre que le titulaire et le mandataire de certification et qui est autorisée par la politique de certification de l'AC ou par contrat avec l'AC à mener certaines actions pour le compte du titulaire (demande de révocation, de renouvellement, …).

Typiquement, dans une entreprise ou une administration, il peut s'agir d'un responsable hiérarchique du titulaire ou d'un responsable des ressources humaines.

Ref_Deliv_Cert_Qual_Exig 15. Les personnes autorisées doivent être clairement identifiées dans la politique de certification de l'autorité de certification, ou par contrat avec celle-ci. Le dossier comportera a minima les documents suivants :

- Une copie de la carte nationale d'identité électronique en cours de validité de la personne autorisée ou tout document valide justifiant son identité (comportant une photo d'identité et délivré par une autorité compétente) ;
- Un document justifiant son statut de personne autorisée.

Ref_Deliv_Cert_Qual_Exig 16. De même, les actions que ces personnes sont autorisées à accomplir pour le compte d'un titulaire doivent être clairement spécifiés politique de certification de l'autorité de certification ou par contrat avec celle-ci.

6.2.4 Vérification de l'identité au vu de la délivrance d'un certificat qualifié

[Précisions relatives aux dispositions du paragraphe 1 de l'alinéa 2 de l'article 33 de la loi n°43-20 ; et aux dispositions de l'article 20 du décret 2.22.687].

En complément du chapitre « 6.2 Identification et authentification » (Identification and authentication) de la norme EN 319 411-2 .

Pour rappel, comme prévu par l'article 33 de la Loi 43-20, la vérification de l'identité de la personne physique ou morale à laquelle le prestataire de service de confiance agréé délivre un **certificat qualifié** doit être réalisée, avant la délivrance dudit certificat, soit :

a. par la **présence en personne** de la personne physique ou du représentant autorisé de la personne morale :

   ➔ ***Vérification de l'identité en présentiel lors d'un face à face physique (a) ;***

b. **à distance,** à l'aide d'un **moyen d'identification électronique** dont la délivrance a nécessité la présence physique de la personne physique ou du représentant autorisé de la personne morale devant l'entité ayant délivré ce moyen :

   ➔ ***Vérification de l'identité à distance à l'aide d'un moyen d'identification électronique (b) ;***

c. au moyen d'un **certificat électronique qualifié** de signature électronique ou de cachet électronique précédemment délivré à une personne dont l'identité a été vérifiée conformément au a) ou b) :

➔ ***Vérification de l'identité*** **au moyen d'un certificat électronique qualifié** *de signature ou de cachet électronique* ***(c) ;***

d. à l'aide **d'autres méthodes d'identification** qui fournissent une **garantie jugée** par l'autorité nationale, **équivalente** aux moyens précités en terme de fiabilité quant à la présence en personne :

➔ ***Vérification de l'identité*** **au moyen d'une méthode d'identification fiable reconnue et attestée par l'Autorité (d).**

Dans le présent chapitre, on désignera par « **Demandeur** » la personne physique ou le représentant autorisé de la personne morale, dont l'identité est vérifiée par le PSCo agréé dans le cadre de la délivrance d'un certificat électronique qualifié.

NB : Comme stipulé au niveau de l'article 33 de la loi n°43-20, par dérogation à l'article 32 de la Loi 43-20, cette vérification de l'identité peut être déléguée par le PSCo agréé à un tiers dans le cadre d'un contrat de sous-traitance liant ce dernier avec le PSCo concerné et approuvé par l'autorité nationale.

Ci-après les exigences et modalités applicables à chacun des (4) schémas de vérification de l'identité (a, b, c, d précitées) dans le cadre de la délivrance d'un certificat qualifié à un demandeur.

Ref_Deliv_Cert_Qual_Exig 17. Quelle que soit la méthode de vérification de l'identité utilisée par le PSCo agréé, les informations relatives à l'identité du demandeur et portées dans le certificat électronique doivent strictement correspondre aux informations portées sur les éléments présentés dans le cadre de la vérification d'identité.

Ref_Deliv_Cert_Qual_Exig 18. Quelle que soit la méthode de vérification de l'identité utilisée, il est entendu que la collecte, le traitement et le cas échéant la conservation des données de vérification de l'identité, devra se faire conformément aux réglementations en vigueur notamment dans le respect strict des dispositions de la loi n°09-08 relative à la protection des données des personnes physiques à l'égard du traitement des données à caractère personnel, et à la délibération en vigueur de la Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel (CNDP).

Ref_Deliv_Cert_Qual_Exig 19. Le PSCo agréé s'engage en particulier à :

- Préserver la sécurité et l'intégrité des données, notamment empêcher qu'elles ne soient déformées, endommagées et empêcher toute utilisation détournée, malveillante ou frauduleuse des données traitées ;
- Empêcher tout accès ou publication qui ne soit pas préalablement autorisé par le demandeur ;
- Ne traiter les données que dans le cadre des instructions et de l'autorisation reçues du demandeur ;
- S'assurer de la licéité des traitements réalisés dans le cadre de la prestation réalisée ;
- Respecter son obligation de secret, de sécurité et de confidentialité, à l'occasion de toute opération de maintenance et de télémaintenance, réalisée au sein des locaux du PSCo agréé ou de toute société intervenant dans le cadre du traitement .

Ref_Deliv_Cert_Qual_Exig 20. Dans le cas où la vérification de l'identité du demandeur est réalisée par un prestataire tiers pour le compte du PSCo agréé dans le cadre d'un contrat de sous-traitance, une approbation préalable de l'autorité nationale est obligatoire. Les dispositions et exigences relatives à la vérification d'identité s'appliquent aussi bien au PSCo qu'au prestataire tiers en question.

(a) Vérification de l'identité en présentiel lors d'un face à face physique

Ref_Deliv_Cert_Qual_Exig 21. Pour une vérification de l'identité dans le cas (a) Vérification de l'identité en présentiel lors d'un face à face physique, le PSCO agréé doit se conformer :

- Aux exigences de la **clause 9.2.1** du standard **ETSI TS 119 461** dans le cas d'une personne physique ;
- Complétées par les exigences de la **clause 9.4** dans le cas d'un représentant autorisé d'une personne morale en se restreignant à l'application de la clause 9.2.1 dans le cadre de l'exigence *USE-9.4-01 ;*

Ref_Deliv_Cert_Qual_Exig 22. La personne physique ou le représentant autorisé par la personne morale, devra présenter un document officiel d'identité avec photographie (exemple carte nationale d'identité, la carte de séjour …) au PSCo agréé en charge de la vérification.

Ref_Deliv_Cert_Qual_Exig 23. La vérification du document officiel d'identité présenté doit permettre de s'assurer :

- Que le document présenté est en cours de validité ;
- Que ledit document n'est pas déclaré volé ou révoqué par une source disponible publiquement ;
- Que le visage du demandeur correspond à la photographie portée sur le document officiel d'identité présenté ;
- Que les informations énoncées par le demandeur (nom, date de naissance...) correspondent aux informations portées sur le document ;
- Que ce document ne semble pas contrefait et ne présente pas de signe de falsification.

Ref_Deliv_Cert_Qual_Exig 24. La vérification de l'authenticité du document d'identité présenté par le demandeur doit se faire a minima au moyen d'une inspection physique (tactile et visuelle) des caractéristiques de sécurité de ce document. Parmi les exemples de caractéristiques de sécurité figurent les hologrammes, les filigranes, les encres, la micro-impression, etc. (par exemple, le site ww.cnie.ma liste certains points de contrôle relatifs à la CNIE).

Ref_Deliv_Cert_Qual_Exig 25. Une procédure de vérification de l'authenticité du document d'identité doit être élaborée, documentée et partagée avec l'ensemble des agents qui procèdent à la vérification. La procédure doit notamment lister les points de contrôle, les éléments à vérifier (notamment visuels) et la méthode de vérification. Le PSCo agréé doit s'assurer que cette procédure est utilisée systématiquement dans le cadre de la vérification de l'authenticité du document d'identité présenté par le demandeur.

Ref_Deliv_Cert_Qual_Exig 26. La vérification physique de l'identité du demandeur peut être différée mais devra se produire dans tous les cas avant la délivrance du certificat qualifié par l'agent d'enregistrement au demandeur.

(b) Vérification de l'identité à distance à l'aide d'un moyen d'identification électronique

Pour rappel, l'article 20 du décret 2.22.687, établit qu'il est entendu par moyens d'identification électronique au sens du (b) du paragraphe 1 de l'alinéa 2 de l'article 33 de la loi n° 43-20 précitée :

- La carte nationale d'identité électronique, régie par les dispositions de la loi n° 04-20 relative à la carte nationale d'identité électronique ;
- Tout autre document électronique qui permet, conformément au texte législatif ou réglementaire qui l'institue, de prouver l'identité à distance de son titulaire et qui répond aux spécifications techniques minimales fixées par l'autorité nationale.

Ref_Deliv_Cert_Qual_Exig 27. Pour une vérification de l'identité dans le cas du schéma (b) (Vérification de l'identité à distance à l'aide d'un moyen d'identification électronique) le PSCO agréé doit se conformer aux exigences des **clauses 8.2.3, 8.3.2 et 9.2.4** du standard **ETSI TS 119 461** pour les usages relatifs aux documents d'identité électronique (digital identity document) et autres moyens eID (eID means).

Ref_Deliv_Cert_Qual_Exig 28. Ne peut être utilisé comme moyen d'identification électronique dans le cadre du schéma de vérification (b) qu'un document d'identité électronique au sens de l'article 20 du décret 2.22.687 respectant les dispositions suivantes :

- Délivré sous une forme exploitable par une machine (typiquement documents eMRTD relativement à ICAO 9303-10) ;
- Signé/cacheté électroniquement par l'émetteur ;
- Dont l'authenticité peut être vérifiée de manière cryptographique à l'aide d'un composant de sécurité du document ;
- Permettant une authentification multi-facteurs (au moins 2 facteurs de natures différentes).

Ref_Deliv_Cert_Qual_Exig 29. Dans le cadre du schéma (b), le PSCO agréé vérifie l'authenticité du document d'identité électronique du demandeur, de manière cryptographique à l'aide du composant de sécurité du document.

Ref_Deliv_Cert_Qual_Exig 30. Les informations d'identité du demandeur (attributs) présentes sur le document d'identité et collectés dans le cadre de la vérification d'identité, doivent être extraite directement du composant de sécurité dudit document.

Ref_Deliv_Cert_Qual_Exig 31. Le schéma de vérification (b) doit permettre d'établir que le demandeur est bien le titulaire légitime du moyen d'identification qu'il présente. Le demandeur devra a minima s'authentifier avec deux facteurs de natures différentes, pour démontrer son lien avec le moyen d'identification électronique qu'il soumet.

Ref_Deliv_Cert_Qual_Exig 32. Le PSCo agréé doit protéger en confidentialité et en intégrité les données d'identification échangées entre le point de collecte des données du côté du demandeur (exemple : application sur le smartphone du demandeur...) et le service de vérification d'identité à distance.

Ref_Deliv_Cert_Qual_Exig 33. Si le procédé de vérification de l'identité nécessite l'utilisation d'une application spécifique du côté du demandeur ou du prestataire (notamment pour collecter/lire les données d'identification à partir du moyen d'identification, procéder à l'authentification du demandeur, vérifier l'authenticité du document...), celle-ci devra :

- Être certifiée Common Criteria EAL2 ou équivalent (équivalence validée par l'autorité nationale) ;
- Disposer de mécanismes permettant de limiter le risque de son altération ou de sa substitution ;
- Disposer de moyens permettant de garantir son authenticité (contrôle d'intégrité, signature du fournisseur...) ;
- Être mise à disposition des utilisateurs à partir de magasins d'applications sécurisés, reconnus ou sur le site officiel du prestataire de service avec un lien de téléchargement bien identifié. Le PSCo devra s'assurer qu'une veille régulière est bien réalisée pour détecter la mise à disposition d'applications frauduleuses visant à se substituer à l'application officielle.

Ref_Deliv_Cert_Qual_Exig 34. Le PSCo agréé devra s'assurer de la création systématique d'un dossier de preuve de vérification d'identité intégré au dossier d'enregistrement. Il comprendra a minima :

- Les données d'identification du demandeur, acquises par le procédé de vérification d'identité ;
- Les constats intermédiaires issus des traitements automatisés (et/ou humains) de la vérification des données d'identification ;
- Les résultats des traitements de vérification d'établissant ou non la correspondance entre le demandeur et le moyen d'identification qu'il a présenté.

Ref_Deliv_Cert_Qual_Exig 35. Le dossier de preuve de vérification de l'identité à distance doit être protégé en confidentialité et en intégrité.

(c) Vérification de l'identité au moyen d'un certificat électronique qualifié de signature ou de cachet électronique

Ref_Deliv_Cert_Qual_Exig 36. Pour une vérification de l'identité du demandeur selon le schéma (c) (vérification de l'identité au moyen d'un certificat qualifié de signature/cachet électronique) la demande de certificat doit être réalisée de façon numérique et déposée électroniquement auprès du PSCo. Elle doit comporter l'ensemble des informations nécessaires à la délivrance du certificat et doit démontrer la manifestation du consentement du demandeur pour la délivrance du certificat.

Ref_Deliv_Cert_Qual_Exig 37. Cette demande de certificat doit être :

- Signée électroniquement par le demandeur, a minima à l'aide d'une signature électronique avancée reposant sur un certificat qualifié ;
- ou Cachetée électroniquement à l'aide d'un cachet électronique avancé reposant sur un certificat qualifié.

Ref_Deliv_Cert_Qual_Exig 38. Le PSCo agréé doit s'assurer que le certificat qualifié, utilisé pour la signature électronique ou le cachet électronique de la demande de certificat qualifié, a été délivré selon l'un des deux schémas de vérification d'identité (a) Vérification de l'identité en présentiel lors d'un face à face physique ou (b) Vérification de l'identité à distance à l'aide d'un moyen d'identification électronique, décrits précédemment.

Ref_Deliv_Cert_Qual_Exig 39. L'application du schéma de vérification de l'identité (c) n'est valable qu'une fois pour un unique renouvellement du certificat électronique qualifié. Lors du second renouvellement, en revanche, la vérification de l'identité devra être réalisée selon les mêmes modalités que la délivrance initiale suivant l'un des schémas (a), (b) ou (d).

Ref_Deliv_Cert_Qual_Exig 40. La signature électronique avancée ou le cachet électronique avancé utilisé par le demandeur doit respecter doit respecter les formats autorisés précisés dans [Ref_PSCo_AG], à savoir :

- PAdES conformément à la norme ETSI EN 319 142-1 ;
- XAdES conformément à la norme ETSI EN 319 132-1 ;
- CAdES conformément à la norme ETSI EN 319 122-1 ;

Pour les conteneurs associés :

- ASiC conformément à la norme ETSI EN 319 162-1.

Ref_Deliv_Cert_Qual_Exig 41. La signature ou le cachet électronique avancée utilisé par le demandeur doit faire l'objet d'un horodatage (de préférence qualifié) permettant de garantir sa date présumée de création.

Ref_Deliv_Cert_Qual_Exig 42. Le PSCo agréé doit mettre en œuvre un processus de validation de la signature ou du cachet répondant aux dispositions prévues par l'article 10 de la Loi 43-20 à

l'exception du point 6 qui n'est pas obligatoire ici (la signature électronique en question ici ne repose pas nécessairement sur un dispositif qualifié), appliquées *mutatis mutandis* pour le cachet.

(d) *Vérification de l'identité* au moyen d'une méthode d'identification fiable reconnue et attestée par l'Autorité

Quelques différences à noter par rapport au schéma (b) :

- Le schéma (d) évoque des méthodes d'identification quand le (b) se base sur des moyens d'identification ;
- Une méthode d'identification peut utiliser à un moyen d'identification ;
- Le moyen d'identification utilisé dans le schéma (b) nécessite préalablement un face à face physique en présentiel ;
- La liste des moyens d'identification utilisables dans le schéma (b) est préétablie (l'article 20 du décret 2.22.687).

Ref_Deliv_Cert_Qual_Exig 43. Pour une vérification de l'identité du demandeur conformément au schéma (d) *Vérification de l'identité au moyen d'une méthode d'identification fiable reconnue et attestée équivalente par l'Autorité* ; des procédés et moyens technologiques fiables et sécurisés devront être mis en œuvre afin d'assurer l'équivalence à la présence physique aux fins de l'identification du demandeur. Cela inclut notamment :

- La collecte sécurisée de données d'identification du demandeur (liveness, face à face distant...) incluant nécessairement l'utilisation d'une preuve d'identité reconnue ;

  (Une preuve d'identité reconnue peut être un document valide justifiant de l'identité comportant une photo d'identité et délivré par une autorité compétente ; ou des éléments immatériels d'identification reconnus par l'Etat, des identifiants associés à un registre reconnu de confiance…) ;
- La vérification des données d'identification utilisée et la validation de l'authenticité de la preuve d'identité par le biais de traitements automatisés fiables (éventuellement complétés par des traitements humains) ;
- La vérification que le demandeur est bien le titulaire légitime de l'élément d'identification qu'il utilise et que l'élément d'identité utilisé est bien en la possession du demandeur ;
- La constitution du dossier de preuve de vérification de l'identité ;
- La mise en œuvre de moyens de contrôle devant atténuer les risques de fraude et/ou d'usurpation de l'identité ;
- La mise en œuvre de mesures assurant la protection en confidentialité et en intégrité des données à caractère personnel d'identification de l'utilisateur conformément aux dispositions légales et réglementaires en vigueur.

Le respect du standard **ETSI TS 119 461** notamment les clauses référencées au niveau de son annexe A3 et la couverture des risques listés en son annexe B ; permet d'apporter une présomption de conformité à cette exigence.

D'autres méthodes peuvent être utilisées, sous réserve que l'autorité nationale atteste de leur équivalence, en termes de garantie, avec la présence physique en personne.

Ref_Deliv_Cert_Qual_Exig 44. Si le service nécessite l'installation d'une application spécifique du côté du demandeur, celle-ci doit disposer de mécanismes permettant de limiter le risque de son altération ou de sa substitution. Elle doit être par ailleurs au moins certifiée Common Criteria EAL2 ou équivalent (équivalence validée par l'autorité)

Ref_Deliv_Cert_Qual_Exig 45. La mise en œuvre d'une vérification de l'identité conformément au schéma (d) est soumise à un accord préalable de l'autorité nationale :

- Le PSCo souhaitant mettre en œuvre une vérification de l'identité conformément au schéma (d) doit au préalable soumettre à l'autorité un dossier descriptif des moyens et procédés qu'ils souhaitent mettre en œuvre démontrant notamment le respect des exigences précitées, accompagné d'une analyse de risque couvrant notamment les menaces listées au niveau de l'annexe B dudit standard ETSI TS 119 461.

6.2.5 Cumul des usages de clés

Ref_Deliv_Cert_Qual_Exig 46. Un certificat électronique qualifié est destiné à un type d'usage spécifique. Les usages des clés à spécifier dans le certificat sont comme suit :

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

6.2.6 Durée de validité du certificat et des clés

Ref_Deliv_Cert_Qual_Exig 47. La date de fin de validité d'un certificat qualifié ne peut en aucun cas être postérieure à la date de fin de validité du certificat de l'autorité de certification émettrice.

Ref_Deliv_Cert_Qual_Exig 48. La fin de validité d'un certificat d'AC doit être postérieure à la fin de vie des certificats qu'elle émet. La durée de vie des clés d'AC doit être précisée dans sa PC et doit être cohérente avec les caractéristiques des algorithmes et les longueurs de clés utilisés conformément aux exigences relatives aux algorithmes et mécanismes cryptographiques précisées au niveau de [Ref_PSCo_AG].

Ref_Deliv_Cert_Qual_Exig 49. La durée maximale de validité des bi-clés correspondant aux certificats qualifiés de signature électronique et de cachet électronique :

- Doit être fixée en fonction de la taille de clé, conformément à la clause 9.3 du standard [TS_119_312] (comme indiqué dans [Ref_PSCo_AG]) ;
- Ne doit en aucun cas excéder 3 ans.

Ref_Deliv_Cert_Qual_Exig 50. La durée maximale de validité des bi-clés correspondant aux certificats d'authentification de site internet n'excède pas 1 an.

Ref_Deliv_Cert_Qual_Exig 51. La suspension temporaire des certificats qualifiés de signature électronique, de cachet électronique et d'authentification de site internet, est interdite.

6.2.7 CRL et OCSP

Ref_Deliv_Cert_Qual_Exig 52. Il est fortement recommandé de mettre un œuvre un répondeur OCSP, en particulier si le prestataire de service de confiance émet des certificats d'authentification de site internet. Si le prestataire de service de confiance ne met pas en œuvre de répondeur OCSP, alors il doit obligatoirement assurer la publication, l'accessibilité et le maintien à jour d'une liste de certificat révoqués (CRL).

Ref_Deliv_Cert_Qual_Exig 53. Dans le cas où le prestataire de service de confiance met à disposition le statut de révocation des certificats à la fois via la publication d'une CRL 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].

6.2.8 Accessibilité au statut de révocation

Ref_Deliv_Cert_Qual_Exig 54. Le PSCo agréé doit assurer la disponibilité du statut de révocation à tout moment et au-delà de la période de validité du certificat.

Après l'expiration du certificat

Ref_Deliv_Cert_Qual_Exig 55. Dans le cas où le PSCo agréé assure la publication d'une CRL, celle-ci devra obligatoirement respecter les points suivants :

- Comporter l'extension « ExpiredCertsOnCRL », comme prévu par la recommandation ITU-T X.509 ;
- Contenir les numéros de série de l'ensemble des certificats révoqués, y compris les certificats étant arrivés à expiration après leur révocation.

Ref_Deliv_Cert_Qual_Exig 56. Si le PSCo agréé met en œuvre un répondeur OCSP, celui-ci devra obligatoirement respecter les points suivants :

- 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 ;
- Maintenir disponible le statut de révocation du certificat après son expiration.

Si la clé de l'AC émettrice du certificat qualifié est sur le point d'expirer

Ref_Deliv_Cert_Qual_Exig 57. Si la clé de l'AC émettrice du certificat qualifié est sur le point d'expirer alors :

- Tous les certificats non-expirés émis par cette AC doivent être révoqués ;
- Si le PSCo assurait la publication d'une CRL, une dernière CRL devrait être publiée. Celle-ci ayant une fin de validité positionnée au 31 décembre 9999, 23h59m59s ;
- Si le PSCo 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.

6.2.9 Cohabitation de certificats qualifiés et non qualifiés

Ref_Deliv_Cert_Qual_Exig 58. En cas de délivrance de certificats non qualifiés par le PSCo agréé fournissant des certificats qualifiés, il est nécessaire de s'assurer que ces certificats non qualifiés ne comportent pas d'attributs pouvant les faire considérer de manière erronée comme des certificats qualifiés. Plus globalement, le PSCo agréé doit garantir la distinction sans aucune ambiguïté entre les certificats qualifiés et les certificats non qualifiés qu'il fournit notamment lorsqu'ils sont délivrés par une même autorité de certification.

6.2.10 Profils et contenus des certificats qualifiés

Ce paragraphe et les annexes associées précisent les profils type de certificat avec les champs et extensions minimum à retrouver et les indications à respecter concernant leurs valeurs.

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

Ref_Deliv_Cert_Qual_Exig 59. Un PSCo agréé fournissant des certificats qualifiés est tenu de respecter le profil type et le contenu du certificat tels que détaillés en Annexe du présent document,

selon l'usage du certificat qualifié (signature électronique, cachet électronique ou authentification de sites Internet).

Il s'agit des champs et extensions minimums à respecter. Toutefois, les certificats peuvent contenir d'autres champs ou extensions que ceux définis en annexe, en conformité avec la [RFC 5280].

6.2.11 Profil de la liste CRL

Ref_Deliv_Cert_Qual_Exig 60. La liste de certificat révoqué (CRL) publiée par le PSCo agréé doit respecter le profil type et le contenu CRL tels que détaillés en Annexe du présent document.

6.2.12 Profil OCSP

Ref_Deliv_Cert_Qual_Exig 61. Dans le cas où le PSCo agréé met en œuvre un répondeur OCSP, ce dernier devra respecter le profil type OCSP tel que spécifié en Annexe du présent document.

6.2.13 Cessation d'activité

Ref_Deliv_Cert_Qual_Exig 62. En cas de cessation d'activité d'un PSCo agréé fournissant un service de délivrance de certificats qualifiés, et à défaut de garantir la reprise de ses activités par un autre prestataire assurant un niveau équivalent de qualité et de sécurité, le PSCo doit maintenir ou transférer, à un PSCo tiers fiable l'ensemble des moyens permettant d'assurer la continuité des fonctions critiques a minima la fonction de révocation des certificats (accessibilité à la CRL, maintien à jour de la CRL, continuité du service de révocation pour les titulaires des certificats…).

Ref_Deliv_Cert_Qual_Exig 63. Dans le cas où le PSCo agréé cesse de fournir le service de délivrance de certificats qualifié sans pouvoir transférer les fonctions critiques spécifiques du service concerné, vers un autre PSCo tiers qualifié fiable, les exigences ci-dessous s'appliquent :

- Tous les certificats non-expirés émis doivent être révoqués dans un délai maximum de deux (2) mois après en avoir averti les titulaires et l'autorité ;
- Si le PSCo assurait la publication d'une CRL, une dernière CRL devrait être publiée, celle-ci ayant une fin de validité positionnée au 31 décembre 9999, 23h59m59s ;
- Si le PSCo 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 ;
- Les CRL et/ou réponses OCSP produites par le PSCo doivent être mises à disposition des clients du PSCo dans des conditions permettant de garantir leur intégrité.

6.2.14 Conservation des données

[Précisions relatives aux dispositions de l'article 18 du décret 2.22.687]

Ref_Deliv_Cert_Qual_Exig 64. Le PSCo agréé fournissant un service de délivrance de certificats qualifiés est tenu de conserver toutes les informations pertinentes concernant les données délivrées et reçues dans le cadre de la délivrance de certificats qualifiés, notamment afin de pouvoir assurer le service et le cas échéant fournir des preuves suffisantes en cas de litige.

Ref_Deliv_Cert_Qual_Exig 65. Le PSCo agréé conservera a minima les données spécifiées au niveau des clauses 6.4.5 et 6.4.6 de la norme EN 319 411-2 en complément des éléments précisés dans [Ref_PCSo_AG]. Cela comprend notamment :

- Les Dossiers d'enregistrement y compris les dossiers de preuve vérification de l'identité des demandeurs, les justificatifs d'identité des titulaires des certificats et, le cas échéant, de leurs entités de rattachement… ;
- Les mandats et attestations d'engagement dans le cas du recours à un mandataire ;

- Une attestation d'engagement ;
- Les PC (Politiques de Certification) et les DPC (Déclaration des Pratiques de Certification)
- Les récépissés ou notifications (à titre informatif)
- Les certificats et CRL tels qu'émis ou publiés ;
- Les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- Les accords contractuels avec d'autres PSCo ou des prestataires tiers intervenants dans la délivrance des certificats qualifiés (typiquement, le cas échéant, les contrats éventuels avec des prestataires tiers réalisant la vérification de l'identité des demandeurs lors de la phase d'enregistrement) ;
- Les journaux d'événements (logs) et pistes d'audit générées par les différentes composantes de la PKI (tels que précisés au niveau de la norme EN 319 411-2).

Ref_Deliv_Cert_Qual_Exig 66. Le PSCo agréé doit conserver ces données précisées et maintenir l'accessible pour les personnes autorisées, pendant une période minimale de sept (7) **ans** après la fin de validité du certificat qualifié objet de la demande, et ce y compris après un éventuel arrêt d'activité.

Ref_Deliv_Cert_Qual_Exig 67. Le PSCo agréé précisera dans ses conditions générales d'utilisation, la durée de conservation appliquée (7 ans minimum) ainsi que, le cas échéant, les modalités de réversibilité et de portabilité.

6.2.15 Modules cryptographiques utilisés

Ref_Deliv_Cert_Qual_Exig 68. Les modules cryptographiques utilisés pour réaliser les fonctions ci-après doivent impérativement être conformes aux dispositions relatives aux modules cryptographiques spécifiées au niveau du référentiel [Ref_PSCo_AG] :

- Signature des certificats des autorités de certification ;
- Signature des certificats des demandeurs ;
- Signature des réponses OCSP et les CRL ;
- Génération des clés privées des autorités de certification ;
- Génération des clés privées des demandeurs le cas échéant.

6.2.16 Publication sur la liste nationale des PSCo agréés

[Précisions relatives aux dispositions de l'article 53 – Loi n°43-20]

Ref_Deliv_Cert_Qual_Exig 69. L'identification d'un service de délivrance de certificats qualifiés dans la Liste Nationale des PSCo Agréés (LNPA) doit respecter les exigences définies dans [Ref_PSCo_AG].

Ref_Deliv_Cert_Qual_Exig 70. L'identification d'un service de délivrance de certificats qualifiés dans la Liste Nationale des PSCo Agréés (LNPA) se fait au moyen du certificat électronique de l'autorité de certification (AC) qui délivre les certificats en question. Cette AC peut être racine, intermédiaire ou terminale.

Ref_Deliv_Cert_Qual_Exig 71. En particulier, dans le cas d'une AC délivre des certificats qualifiés et des certificats non qualifiés, l'identification doit permettre de distinguer sans ambiguïté les certificats qualifiés qu'elle délivre. Il est recommandé que l'AC utilisée pour l'identification du service de délivrance de certificats qualifiés soit une AC (terminale) qui délivre uniquement des certificats qualifiés.

7 Cas de la création de signature électronique qualifiée à distance

Cas d'usage d'un certificat qualifié QCP-n-QSCD au sens de la norme EN 319 411-2.

Dans le cas où le PSCo souhaite fournir un service de création de signature électronique qualifiée à distance, il doit obligatoirement se conformer aux dispositions ci-dessous

Une signature qualifiée à distance est une signature qualifiée au titre de l'article 6 de la loi 43-20 présentant les spécificités suivantes :

(1) Les données de création de signature ou de cachet électronique sont gérées par un PSCo agréé [Ref_PSCo_AG] pour le compte de l'utilisateur ;

(2) La délivrance du certificat qualifié de signature (QCP-n-QSCD) se fait conformément aux exigences du référentiel [Ref_Deliv_Cert_Qual] ;

(3) Le dispositif qualifié de création de signature électronique (QSCD) utilisé se base sur un module cryptographique certifié Certification EAL4+ (ou supérieur) augmentée de AVA_VAN.5 selon le profil de protection **CEN EN 419 221-5** « Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services » ou équivalent) ;

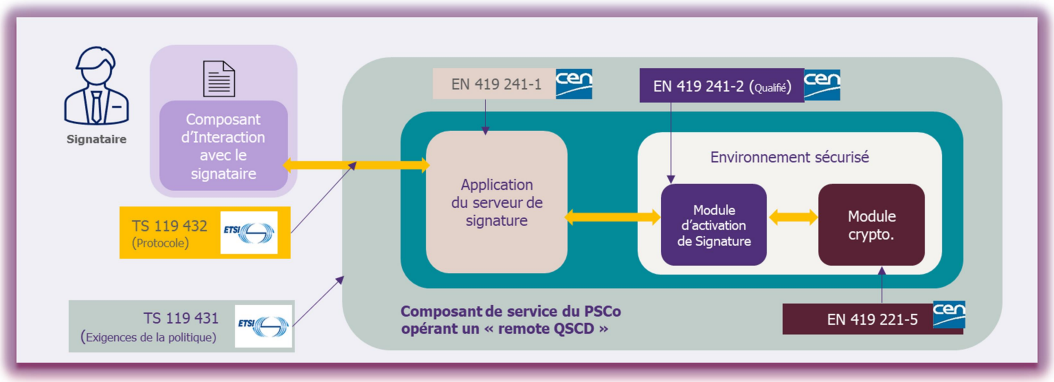
(4) Le respect des exigences des normes suivantes concernant la sécurisation et la fiabilisation du serveur de signature et de l'environnement d'exécution :

- [Norme] **EN 419 241 -1** Trustworthy Systems Supporting Server Signing — Part 1: General System Security Requirements ;
- [Norme] **EN 419 241 -2** Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing ;

(5) La conformité aux exigences du niveau 2 de garantie de contrôle exclusif (**SCAL2**) précisées au niveau des normes **EN 419 241-1** et **EN 419 241-1-2,** qui permet d'atteindre le même niveau de garantie de contrôle exclusif qui serait atteint par un QSCD délivré à l'utilisateur :

- Les clés de signature sont utilisées, avec un niveau de confiance élevé, sous le contrôle exclusif du signataire ;
- L'utilisation de ses clés de signature par le signataire autorisé est imposée par le module d'activation de signature au moyen des données d'activation de signature ; avec une authentification forte multi-facteurs sur la base au moins de 2 facteurs de natures différentes.

Le schéma ci-après (*source ETSI TS 119 431*) synthétise les différentes normes et standard applicables dans le cadre d'une création à distance de signature électronique qualifiée.



NB : Le respect des standards TS 119 432 et TS 119 431 est fortement recommandée.

Rappel : Conformément au référentiel [Ref_PSCo_AG], les formats de signature (ou cachet) électronique autorisés sont :

- PAdES conformément à la norme ETSI EN 319 142-1 ;
- XAdES conformément à la norme ETSI EN 319 132-1 ;
- CAdES conformément à la norme ETSI EN 319 122-1 ;

Pour les conteneurs de signature (ou cachet) électronique :

- ASiC conformément à la norme ETSI EN 319 162-1.

8 Annexes

8.1 Profils et contenus des certificats qualifiés

8.1.1 Profil et contenu du certificat qualifié de signature électronique

Le tableau ci-après précise le profil (champs et extensions) et les informations/valeurs à retrouver au niveau du certificat qualifié destiné à la signature électronique. Les certificats peuvent contenir d'autres champs ou extensions que ceux définis ci-dessous, en conformité avec la [RFC 5280].

<table>
<tr><th>Champ</th><th>Détail et valeur</th></tr>
<tr><td>Version</td><td>2 (=version 3)</td></tr>
<tr><td>Serial number</td><td>Numéro de série unique, dans le domaine de confiance auquel appartient le certificat, qui l'identifie de façon unique</td></tr>
<tr><td>Signature Algorithm</td><td>Identifiant du procédé utilisé par l'AC pour signer le certificat</td></tr>
<tr><td>Issuer</td><td>
<table>
<tr><th>Attributs</th><th>Détails et valeurs</th></tr>
<tr><td>CountryName</td><td>C=MA
(2 caractères code pays Maroc conforme ISO 3166-1)</td></tr>
<tr><td>OrganizationName</td><td>Dénomination officielle ou raison sociale du prestataire telle qu'enregistrée auprès des autorités compétentes et telle que déclarée auprès de l'Autorité nationale</td></tr>
<tr><td>OrganizationIdentifier</td><td>Numéro d'immatriculation officiel du prestataire conformément à [EN_319_412-1] Clause 5.1.4 (ICE, numéro d'inscription au registre du commerce, …)
Exemple « NTRMA-Numéro registre de commerce »</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>notBefore</td><td>Date de début de validité du certificat</td></tr>
<tr><td>noteAfter</td><td>Date de fin de validité du certificat</td></tr>
<tr><td>Subject</td><td>
<table>
<tr><th>Attributs</th><th>Détail et valeurs</th></tr>
<tr><td>countryName</td><td>Nom du pays d'activité du titulaire ou de l'entité dont il dépend (si le certificat est délivré à une personne physique dans le cadre de son appartenance à une entité donnée) et dans lequel les autres attributs du champ « Subject » doivent être interprétés.

Valeur = 2 caractères code pays conforme ISO 3166-1</td></tr>
<tr><td>organizationName</td><td>(Obligatoire si le certificat est délivré au titulaire dans le cadre de son appartenance à une entité donnée, interdit sinon)
Dénomination officielle ou raison sociale de l'entité dont dépend le titulaire du certificat telle qu'enregistrée auprès des autorités compétentes et telle que déclarée auprès de l'Autorité nationale.</td></tr>
<tr><td>organizationIdentifier</td><td>(Obligatoire si le certificat est délivré au titulaire dans le cadre de son appartenance à une entité donnée, interdit sinon)
Numéro d'immatriculation officiel de l'entité dont dépend le titulaire du certificat, conformément à [EN_319_412-1] Clause 5.1.4 (ICE, numéro d'inscription au registre du commerce, …)
Exemple « NTRMA-Numéro registre de commerce »</td></tr>
<tr><td>serialNumber</td><td>(Optionnel) Elément complémentaire permettant de distinguer les homonymes</td></tr>
<tr><td colspan="2">Les 3 attributs suivants (givenName, surname et commonName) sont à considérer dans le cas de l'utilisation des informations de l'état civil du titulaire</td></tr>
<tr><td>givenName</td><td>Prénom de l'état civil du titulaire du certificat</td></tr>
<tr><td>surname</td><td>Nom de l'état civil du titulaire du certificat</td></tr>
<tr><td>commonName</td><td>Prénom indiqué dans givenName, suivi d'un espace, suivi du Nom indiqué dans surname (ou une autre façon pour indiquer le nom et prénom du titulaire tel qu'il devrait être affiché par les applications)</td></tr>
</table>
</td></tr>
</table>

	Les 2 attributs suivants (Pseudonym et commonName) sont à considérer dans le cas de l'utilisation d'un Pseudonyme du titulaire du certificat	
	Pseudonym	Pseudonyme du titulaire du certificat
	commonName	Pseudonyme du titulaire du certificat
Public Key Algorithm	Contient l'algorithme de clé publique conforme à la section relative aux algorithmes et mécanismes cryptographiques du référentiel [Ref_PSCo_AG]	
Public-Key	Contient la valeur de la clé publique du titulaire du certificat	

Extensions	Obligatoire	Détails et valeurs		
Basic Constraints	Oui	"CA:false"		
Certificate Policies	Oui	Identifiant de la Politique de Certification associé		
CRL Distribution Points	Obligatoire si pas d'OCSP	Point de publication des listes de certificats révoqués. En cas d'absence d'un service OCSP, un point de distribution des CRL est requis et le point de publication des CRL doit faire référence à une CRL publiée. Au moins une des CRL publiées doit être accessible selon le protocole http ou LDAP.		
Authority Information Access	Oui	• accessMethod OID = « 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 = « id-ad-ocsp » • accessLocation valorisé avec le chemin d'accès au répondeur OCSP (obligatoire si aucune CRL n'est publiée)		
Key Usage	Oui	" nonRepudiation"		
qcStatements	Oui	Extension	Présente	Détail et valeur
		esi4-qcStatement-1	Oui	Valeur " id-etsi-qcs-QcCompliance" *Indication que le certificat émis est qualifié*
		esi4-qcStatement-2	Optionnel	Extension optionnelle, décrite dans la norme [EN_319_412-5].
		esi4-qcStatement-3	Optionnel	Extension optionnelle, décrite dans la norme [EN_319_412-5].
		esi4-qcStatement-4	Oui	Valeur " id-etsi-qcs-QcSSCD" *Indication que la clé privée correspondante est stockée dans un dispositif sécurisé de création de signature électronique.*
		esi4-qcStatement-5	Optionnel	Extension optionnelle, décrite dans la norme [EN_319_412-5]
		esi4-qcStatement-6	Oui	Valeur "id-etsi-qct-esign" *Indication que le certificat est un certificat qualifié de signature électronique.*
Subject Key Identifier	Oui	Identifiant de la clé publique contenue dans le certificat.		
Authority Key Identifier	Oui	Identifiant de la clé publique de l'AC émettrice		

Tableau 4 : *Profil du certificat qualifié de signature électronique qualifiée (champs de base + extensions)*

8.1.2 Profil et contenu du certificat qualifié de cachet électronique

Le tableau ci-après précise le profil (champs et extensions) et les informations/valeurs à retrouver au niveau du certificat qualifié destiné au cachet électronique. Les certificats peuvent contenir d'autres champs ou extensions que ceux définis ci-dessous, en conformité avec la [RFC 5280].

Champ	Détail et valeur
Version	2 (=version 3)
Serial number	Numéro de série unique, dans le domaine de confiance auquel appartient le certificat, qui l'identifie de façon unique
Signature	Identifiant du procédé utilisé par l'AC pour signer le certificat

<table>
<tr><td>Algorithm</td><td></td></tr>
<tr><td>Issuer</td><td>Identifiant de l'entité ayant signé et délivré le certificat. Conforme à la norme X.501
<table>
<tr><th>Attribut</th><th>Détail et valeur</th></tr>
<tr><td>countryName</td><td>C=MA
(2 caractères code pays Maroc conformes ISO 3166-1)</td></tr>
<tr><td>organizationNAme</td><td>Dénomination officielle ou raison sociale du prestataire telle qu'enregistrée auprès des autorités compétentes et telle que déclarée auprès de l'Autorité nationale</td></tr>
<tr><td>organization Identifier</td><td>Numéro d'immatriculation officiel du prestataire conformément à [EN_319_412-1] Clause 5.1.4 (ICE, numéro d'inscription au registre du commerce, …)
Exemple « NTRMA-Numéro registre de commerce »</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>notBefore</td><td>Date de début de validité du certificat</td></tr>
<tr><td>noteAfter</td><td>Date de fin de validité du certificat</td></tr>
<tr><td>Subject</td><td>
<table>
<tr><th>Attribut</th><th>Détail et valeur</th></tr>
<tr><td>countryName</td><td>Nom du pays d'activité de l'entité titulaire du certificat et dans lequel les autres attributs du champ « Subject » doivent être interprétés.
Valeur = 2 caractères code pays conformes ISO 3166-1</td></tr>
<tr><td>organizationName</td><td>Dénomination officielle ou raison sociale de l'entité titulaire du certificat telle qu'enregistrée auprès des autorités compétentes et telle que déclarée auprès de l'Autorité nationale.</td></tr>
<tr><td>organizationIdentifier</td><td>Numéro d'immatriculation officiel de l'entité titulaire du certificat, conformément à [EN_319_412-1] Clause 5.1.4 (ICE, numéro d'inscription au registre du commerce, …)
Exemple « NTRMA-Numéro registre de commerce »</td></tr>
<tr><td>commonName</td><td>Nom significatif du service mettant en oeuvre le cachet</td></tr>
</table></td></tr>
<tr><td>Public Key Algorithmie</td><td>Contient l'algorithme de clé publique conforme à la section relative aux algorithmes et mécanismes cryptographiques du référentiel [Ref_PSCo_AG]</td></tr>
<tr><td>Public-Key</td><td>Contient la valeur de la clé publique du titulaire du certificat</td></tr>
</table>

Extensions	Obligatoire	Détail et valeur
Basic Constraints	Oui	"CA:false"
Certificate Policies	Oui	Identifiant de la Politique de Certification applicable.
CRL Distribution Points	Obligatoire si pas d'OCSP	Point de publication des listes de certificats révoqués. En cas d'absence d'un service OCSP, un point de distribution des CRL est requis et le point de publication des CRL doit faire référence à une CRL publiée. Au moins une des CRL publiées doit être accessible selon le protocole http ou LDAP.
Authority Information Access	Oui	• accessMethod OID = « 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 = « id-ad-ocsp » • accessLocation valorisé avec le chemin d'accès au répondeur OCSP (obligatoire si aucune CRL n'est publiée)
Key Usage	Oui	" digitalSignature" et/ou "nonRepudiation"
qcStatements	Oui	<table><tr><th>Extension</th><th>Présente</th><th>Détail et valeur</th></tr><tr><td>esi4-qcStatement-1</td><td>Oui</td><td>Valeur " id-etsi-qcs-QcCompliance". Indication que le certificat émis est qualifié</td></tr><tr><td>esi4-qcStatement-2</td><td>Optionnel</td><td>Extension optionnelle, décrite dans la norme [EN_319_ 412-5].</td></tr></table>

		esi4-qcStatement-3	Optionnel	Extension optionnelle, décrite dans la norme [EN_319_ 412-5].
		esi4-qcStatement-4	Oui	Valeur " id-etsi-qcs-QcSSCD". *Indication que la clé privée correspondante est stockée dans un dispositif qualifié de création de cachet électronique.*
		esi4-qcStatement-5	Optionnel	Extension optionnelle, décrite dans la norme [EN_319_ 412-5].
		esi4-qcStatement-6	Oui	Valeur "id-etsi-qct-eseal". *Indication que le certificat est un certificat qualifié de cachet électronique.*
Subject Key Identifier	Oui	Identifiant de la clé publique contenue dans le certificat.		
Authority Key Identifier	Oui	Identifiant de la clé publique de l'AC émettrice		

Tableau 5 : *Profil certificat qualifié pour cachet électronique qualifié (champs de base + extensions)*

8.1.3 Profil et contenu du certificat qualifié d'authentification de sites internet

Le tableau ci-après précise le profil (champs et extensions) et les informations/valeurs à retrouver au niveau du certificat qualifié destiné à l'authentification électronique de sites internet. Les certificats peuvent contenir d'autres champs ou extensions que ceux définis ci-dessous, en conformité avec la [RFC 5280].

Champ	**Détail et valeur**	
Version	2 (=version 3)	
Serial number	Numéro de série unique, dans le domaine de confiance auquel appartient le certificat, qui l'identifie de façon unique	
Signature Algorithm	Identifiant du procédé utilisé par l'AC pour signer le certificat	
Issuer	**Attribut**	**Détail et valeur**
	countryName	C=MA (2 caractères code pays Maroc conformes ISO 3166-1)
	organizationName	Dénomination officielle ou raison sociale du prestataire telle qu'enregistrée auprès des autorités compétentes et telle que déclarée auprès de l'Autorité nationale
	organization Identifier	Numéro d'immatriculation officiel du prestataire conformément à [EN_319_412-1] Clause 5.1.4 (ICE, numéro d'inscription au registre du commerce, …) *Exemple « NTRMA-Numéro registre de commerce »*
	commonName	Nom significatif du prestataire ou du service de délivrance de certificats
notBefore	Date de début de validité du certificat	
noteAfter	Date de fin de validité du certificat	
Subject	**Attribut**	**Détail et valeur**
	countryName	Nom du pays dans lequel est établi le titulaire (si personne morale) ou dans lequel réside le titulaire (si personne physique) Valeur = 2 caractères code pays conformes ISO 3166-1
	localityName	Nom de la ville dans laquelle est établi le titulaire (si personne morale) ou dans lequel réside le titulaire (si personne physique) *Exemple « RABAT »*
	organizationName	*(Obligatoire si le certificat est délivré à une personne morale ou à une personne physique utilisant le certificat dans le cadre de son appartenance à une entité donnée, interdit sinon)* Dénomination officielle ou raison sociale de l'entité titulaire du certificat (ou dont dépend le titulaire personne physique) telle qu'enregistrée auprès des autorités compétentes et telle que déclarée auprès de l'Autorité nationale.
	organizationIdentifier	*(Obligatoire si le certificat est délivré à une personne morale ou à une personne physique utilisant le certificat dans le cadre de son*

		appartenance à une entité donnée, interdit sinon) Numéro d'immatriculation officiel de l'entité titulaire du certificat (ou dont dépend le titulaire personne physique), conformément à [EN_319_412-1] Clause 5.1.4 (ICE, numéro d'inscription au registre du commerce, …) *Exemple « NTRMA-Numéro registre de commerce »*
	commonName	*(Optionnel)* L'un des noms de domaine présents dans l'extension SubjectAltname.
	Les 3 attributs suivants (givenName, surname et serialNumber) concernent un certificat délivré à une personne physique identifié par son état civil	
	givenName	Prénom tel qu'indiqué sur l'état civil du titulaire du certificat
	Surname	Nom tel qu'indiqué sur l'état civil du titulaire du certificat
	serialNumber	*(Optionnel)* Elément complémentaire permettant de distinguer les homonymes (personnes physiques)
	Les 3 attributs suivants (Pseudonym, surname et serialNumber) concernent un certificat délivré à une personne physique identifié par un pseudonyme	
	Pseudonym	Pseudonym du titulaire du certificat
	Surname	Nom tel qu'indiqué sur l'état civil du titulaire du certificat
	serialNumber	*(Optionnel)* Elément complémentaire permettant de distinguer les homonymes (personnes physiques)
Public Key Algorithm	Contient l'algorithme de clé publique conforme à la section relative aux algorithmes et mécanismes cryptographiques du référentiel [Ref_PSCo_AG]	
Public-Key	Contient la valeur de la clé publique du titulaire du certificat	

Extensions	Obligatoire	Détail et valeur
Basic Constraints	Oui	"CA:false"
Certificate Policies	Oui	Identifiant de la Politique de Certification applicable.
CRL Distribution Points	Obligatoire si pas d'OCSP	Point de publication des listes de certificats révoqués. En cas d'absence d'un service OCSP, un point de distribution des CRL est requis et le point de publication des CRL doit faire référence à une CRL publiée. Au moins une des CRL publiées doit être accessible selon le protocole http ou LDAP.
Authority Information Access	Oui	• accessMethod OID = « 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 = « id-ad-ocsp » • accessLocation valorisé avec le chemin d'accès au répondeur OCSP (obligatoire si aucune CRL n'est publiée)
Key Usage	Oui	"digitalSignature" et/ou "keyEncipherment" ou "keyAgreement"
qcStatements	Oui	Extension / Présente / Détail et valeur esi4-qcStatement-1 / Oui / valeur " id-etsi-qcs-QcCompliance". *Indication que le certificat émis est qualifié* esi4-qcStatement-2 / Optionnel / Extension optionnelle, décrite dans la norme [EN_319_ 412-5]. esi4-qcStatement-3 / Optionnel / Extension optionnelle, décrite dans la norme [EN_319_ 412-5]. *esi4-qcStatement-4* / *Non* / *N/A* esi4-qcStatement-5 / Optionnel / Extension optionnelle, décrite dans la norme [EN_319_ 412-5]. esi4-qcStatement-6 / Oui / Valeur "id-etsi-qct-web" *Indication que le certificat est un certificat qualifié d'authentification de site internet.*
Subject Key Identifier	Oui	Identifiant de la clé publique contenue dans le certificat.
Authority Key Identifier	Oui	Identifiant de la clé publique de l'AC émettrice
Subject Alternative Name	Oui	Un ou plusieurs noms de domaine contrôlés par le titulaire

Tableau 6 : *Profil certificat qualifiés d'authentification qualifiée de sites internet (champs de base + extensions)*

8.1.4 Profil et contenu de la liste CRL

La liste de certificat révoqué (CRL) publiée par le PSCo doit respecter le profil type et le contenu CRL ci-après :

Champs de base CRL	Obligatoire	Détail et valeur
Version	Oui	2 (= version 3)
Signature	Oui	Identifiant de l'algorithme utilisé par l'AC pour signer la CRL (L'algorithme doit être conforme aux indications de [Ref_PSCo_AG])
Issuer DN	Oui	DN de l'AC qui a signé la CRL
This Update	Oui	Date et heure UTC de génération de la CRL
Next Update	Oui	Date et heure UTC de la prochaine mise à jour de la CRL
Revoked Certificates	Oui	Liste des numéros de séries des certificats révoqués ainsi que leur date de révocation

Champ extension de la CRL	Obligatoire	Criticité	Détail et valeur
Authority Key Identifier	Oui	Non	Identifiant de la clé publique de l'AC émettrice
CRL Number	Oui	Non	N° de série de la CRL. Incrémenté de 1 à chaque nouvelle CRL.

Tableau 7 : *Profil liste CRL (Champ de base + extensions)*

8.1.5 Profil et contenu OCSP

Le profil du répondeur OCSP doit respecter le standard [RFC_6960]. Les valeurs des extensions doivent obligatoirement respecter le tableau ci-après :

Les extensions			
Extensions	**Obligatoire**	**Critique**	**Détail et valeur**
Basic Constraints	Oui	Non	"CA:false"
Key Usage	Oui	Oui	digitalSignature
Extended Key Usage	Oui	Oui	id-kp-OCSPSigning
Subject Alternative Name	Oui	Non	Un ou plusieurs noms de domaine contrôlés par le demandeur

Tableau 8 : *Profil OCSP - Extensions*

8.2 Liens vers les normes et standards

- **ETSI EN_319_411-1 :** Electronic Signatures and Infrastructures (ESI) ; Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
  - Se référer à la version la plus récente publiée sur le site de l'ETSI **:**

    https://www.etsi.org/deliver/etsi_en/319400_319499/31941101/
  - A titre indicatif, la version la plus récente au moment de la rédaction du présent document est la suivante (v1.3.1) :

    https://www.etsi.org/deliver/etsi_en/319400_319499/31941101/01.03.01_60/en_31941101v010301p.pdf

- **ETSI EN_319_411-2 :** 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.
  - Se référer à la version la plus récente publiée sur le site de l'ETSI :

    https://www.etsi.org/deliver/etsi_en/319400_319499/31941102
  - A titre indicatif, la version la plus récente au moment de la rédaction du présent document est la suivante (v2.4.1) :

    https://www.etsi.org/deliver/etsi_en/319400_319499/31941102/02.04.01_60/en_31941102v020401p.pdf

- **ETSI EN 319 412-1 :** Electronic Signatures and Infrastructures (ESI); Certificate Profiles - Part 1: Overview and common data structures.
  - Se référer à la version la plus récente publiée sur le site de l'ETSI **:**

    https://www.etsi.org/deliver/etsi_en/319400_319499/31941201/
  - A titre indicatif, la version la plus récente au moment de la rédaction du présent document est la suivante (v1.4.4)

    https://www.etsi.org/deliver/etsi_en/319400_319499/31941201/01.04.04_60/en_31941201v010404p.pdf

- **ETSI EN 319 412-2 :** Electronic Signatures and Infrastructures (ESI); Certificate Profiles - Part 2: Certificate profile for certificates issued to natural persons.
  - Se référer à la version la plus récente publiée sur le site de l'ETSI :
    https://www.etsi.org/deliver/etsi_en/319400_319499/31941202
  - A titre indicatif, la version la plus récente au moment de la rédaction du présent document est la suivante (v2.2.1) :

    https://www.etsi.org/deliver/etsi_en/319400_319499/31941202/02.02.01_60/en_31941202v020201p.pdf

- **ETSI EN 319 412-3 :** Electronic Signatures and Infrastructures (ESI); Certificate Profiles - Part 3: Certificate profile for certificates issued to legal persons.
  - Se référer à la version la plus récente publiée sur le site de l'ETSI :

    https://www.etsi.org/deliver/etsi_en/319400_319499/31941203

- A titre indicatif, la version la plus récente au moment de la rédaction du présent document est la suivante (v1.2.1) :

  https://www.etsi.org/deliver/etsi_en/319400_319499/31941203/01.02.01_60/en_31941203v010201p.pdf

- **ETSI EN 319 412-4 :** Electronic Signatures and Infrastructures (ESI); Certificate Profiles - Part 4: Certificate profile for web site certificates.
  - Se référer à la version la plus récente publiée sur le site de l'ETSI **:**

    https://www.etsi.org/deliver/etsi_en/319400_319499/31941204
  - A titre indicatif, la version la plus récente au moment de la rédaction du présent document est la suivante (v1.2.1) :

    https://www.etsi.org/deliver/etsi_en/319400_319499/31941204/01.02.01_60/en_31941204v010201p.pdf

- **ETSI EN 319 412-5 :** Electronic Signatures and Infrastructures (ESI) ; Certificate Profiles - Part 5: QCStatements.
  - Se référer à la version la plus récente publiée sur le site de l'ETSI :

    https://www.etsi.org/deliver/etsi_en/319400_319499/31941205
  - A titre indicatif, la version la plus récente au moment de la rédaction du présent document est la suivante (v2.3.1) :

    https://www.etsi.org/deliver/etsi_en/319400_319499/31941205/02.03.01_60/en_31941205v020301p.pdf

- **[Standard] ETSI TS 119 461 :** Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects.
  - Se référer à la version la plus récente publiée sur le site de l'ETSI :

    https://www.etsi.org/deliver/etsi_ts/119400_119499/119461
  - A titre indicatif, la version la plus récente au moment de la rédaction du présent document est la suivante (v1.1.1) :

    https://www.etsi.org/deliver/etsi_ts/119400_119499/119461/01.01.01_60/ts_119461v010101p.pdf

- **ETSI Drafting Rules** : règles d'interprétation des verbes modaux et auxiliaires utilisés au niveau des exigences des normes et standard ETSI :

  https://docbox.etsi.org/stf/archive/STF473_SatEC_MAMES/STFworkarea/DraftDeliverables/background%20material/ETSI%20Drafting%20Rules%20%5Bexcerpt%20from%2033_directives_may_2014%5D%2BJRmarking.pdf

- Lien officiel vers les normes CEN 419 xxx :

  https://www.en-standard.eu/csn-standards/36-electrical-engineering/3698-processing-and-interchange-of-documents/