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

5

[Ref_Valid_Qual]

Exigences de conformité des prestataires fournissant un service de **validation qualifié de signature et/ou de cachet électronique qualifié**

Suivi des mise à jour du document [Ref_Valid_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.

AdES (Advanced Electronic Signatures) : désigne les signatures électroniques avancées

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).

EAL2 : Evaluation Assurance Level 2 ; 2ème niveau d'assurance d'évaluation (testé structurellement) selon les Critères Communs.

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, protocole internet permettant d'accéder au statut d'un certificat et de vérifier sa validité en temps réel.

Partie utilisatrice : dans le cadre du présent référentiel, il s'agit de toute personne physique ou morale qui fait appel à un service de validation afin de s'assurer de la validité d'une signature électronique qualifiée ou d'un cachet électronique qualifié.

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.

2 Objet et périmètre

Le présent document, désigné par **[Ref_Valid_Qual]**, constitue le référentiel fixant les exigences de conformité à respecter par les PSCo agréés fournissant un **service de validation qualifié de signatures et/ou de cachets électroniques qualifiés** et ce conformément au **cadre légal national** rappelé dans le présent document au niveau du chapitre « Cadre de référence ».

Le respect des exigences des référentiels [Ref_Valid_Qual] & [Ref_PSCo_AG] conditionnent l'obtention de l'agréement pour la fourniture du service de validation qualifié de signatures et/ou de cachets électroniques 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 de 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_Val_Qual]** est :

- 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_Valid_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 :

- **[Standard] TS_119_441** v1.1.1 (2018-08) ou version ultérieure **:** Electronic Signatures and Infrastructures (ESI) ; Policy requirements for TSP providing signature validation services ;

  Définit les exigences normatives relatives aux prestataires de services de confiance fournissant un service de validation de signature.

- **[Norme] EN_319_102-1** v1.3.1 (2021-11) ou version ultérieure **:** Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation – *Clause 5 « Signature validation » + « Annex A » ;*

  Définit les exigences normatives relatives aux prestataires de services de création et de validation de signature (AdES).

  NB : le [Standard] TS_119_441 et la [Norme] EN_319_102-1 adressent aussi bien la validation de signature électronique que la validation de cachet électronique.

- **[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.

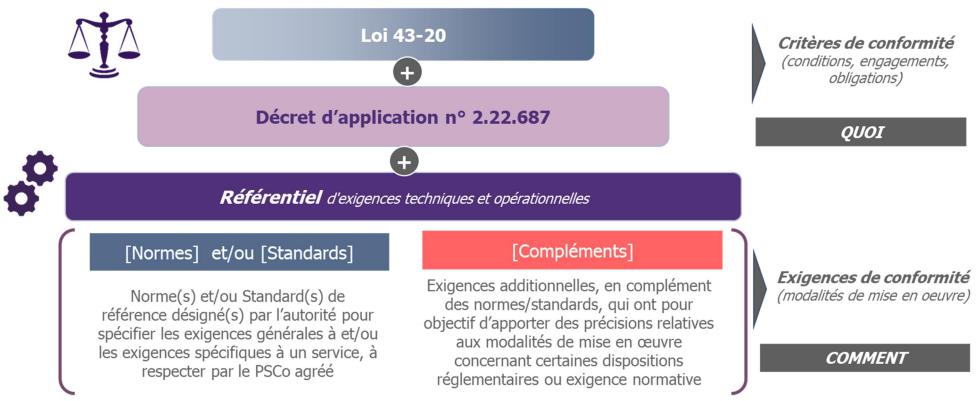

Figure 1 : Structure du cadre juridique et normatif

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 fournis au niveau national ;
- Permettre la reconnaissance à l'international des services fournis 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 » « 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 un service de **validation qualifié** de signatures et/ou de cachets électroniques qualifié, sont consolidés au niveau du tableau suivant :

Chapitre Ier **Section 1ère** *Des service de confiances*	**Article 2**	Définition de la **validation** : Processus de vérification et de confirmation de la validité d'une signature électronique ou d'un cachet électronique.
	Article 10	Conditions de **validation** (confirmation de la validité) d'une **signature électronique qualifiée :** - le certificat sur lequel repose la signature était, au moment de la signature, un certificat qualifié de signature électronique ; – le certificat qualifié délivré par un PSCo agréé était valide au moment de la signature ; – les données de validation de la signature correspondent aux données communiquées à la partie utilisatrice ; – l'ensemble unique de données représentant le signataire dans le certificat est correctement fourni à la partie utilisatrice ; – l'utilisation d'un pseudonyme est clairement indiquée à la partie utilisatrice, si un pseudonyme a été utilisé au moment de la signature ; – la signature électronique a été créée par un dispositif qualifié de création de signature électronique et les conditions de création d'une signature avancée ont été satisfaites ; – l'intégrité des données signées n'a pas été compromise. Le système utilisé pour valider la signature électronique qualifiée doit : - fournir à la partie utilisatrice le résultat correct du processus de validation ; - permettre à la partie utilisatrice de détecter tout problème pertinent relatif à la sécurité.
	Article 11	Critères à respecter par les PSCo pour fournir un service de **validation qualifié** de **signatures** électroniques qualifiées. Un service de validation qualifié des signatures électroniques qualifiées ne peut être fourni que par : - un PSCo **agréé** ; - qui fournit une validation conformément aux dispositions de l'article 10 rappelées ci-avant ; - et permet à la partie utilisatrice de recevoir le résultat du processus de validation d'une manière automatisée, fiable, efficace et portant la signature électronique avancée ou le cachet électronique avancé dudit PSCo.
	Article 19	Conditions de **validation** (confirmation de la validité) d'un **cachet électronique qualifié :** - le certificat sur lequel repose le cachet était, au moment de sa création, un certificat qualifié de cachet électronique ; – le certificat qualifié délivré par un PSCo agréé était valide au moment de la création du cachet ; – les données de validation du cachet correspondent aux données communiquées à la partie utilisatrice ; – l'ensemble unique de données représentant le créateur du cachet dans le certificat est correctement fourni à la partie utilisatrice ; – le cachet électronique a été créé par un dispositif qualifié de création de cachet électronique et les conditions de création d'un cachet avancé ont été satisfaites ; – l'intégrité des données cachetées n'a pas été compromise. Le système utilisé pour valider le cachet électronique qualifié doit : - fournir à la partie utilisatrice le résultat correct du processus de validation ; - permettre à la partie utilisatrice de détecter tout problème pertinent relatif à la sécurité.
	Article 20	Critères à respecter par les PSCo pour fournir un service de **validation qualifié** de **cachets électroniques** qualifiés : Un service de validation qualifié de cachets électroniques qualifiés ne peut être fourni que par : - un PSCo agréé ; - qui fournit une validation conformément à l'article 19 rappelées ci-avant ; - et permet à la partie utilisatrice de recevoir le résultat du processus de validation d'une manière automatisée, fiable, efficace et portant sa signature électronique avancée ou son cachet électronique avancé.

Chapitre Ier **Section II** Des prestataires de service de confiances	**Article 32**	Obligation d'agréement : seuls les PSCo agréés peuvent fournir un service* de confiance qualifié et gérer les opérations y afférentes. * ici service de validation qualifié de signature et/ou cachet électronique qualifié
	Article 33	Utilisation, dans le cadre de la fourniture du service* de confiance qualifié, de systèmes, matériels et logiciels fiables ; et garantie de leur sécurité technique et de la fiabilité des processus pris en charge. * ici service de validation qualifié de signature et/ou cachet électronique qualifié.
	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 service de validation qualifié de signature et/ou cachet électronique 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 personnelles * ici service de validation qualifié de signature et/ou cachet électronique qualifié.

Tableau 1: *Récapitulatif des principaux articles et dispositions de la loi 43-20 relatifs au service de validation qualifié de signature/cachet électroniques 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 un service de **validation qualifié** de signatures et/ou de cachets électroniques qualifiés, sont consolidés au niveau du tableau suivant :

Chapitre Ier **Section Ière** Des services de confiance qualifiés	**Article 2**	Informations (attributs) contenues dans un certificat qualifié de signature et qui permettent de vérifier la validité de cette dernière, notamment : - l'indication du début et de la fin de la durée de validité du certificat ; - l'emplacement des services permettant de s'informer du statut de validité du certificat ; - mention indiquant que le certificat est un certificat qualifié de signature électronique ; - mention indiquant l'utilisation d'un dispositif qualifié de création de signature électronique ; - la signature électronique avancée ou le cachet électronique avancé du PSCo ; ….
	Article 3	Informations (attributs) contenues dans un certificat qualifié de cachet et qui permettent de vérifier la validité du cachet électronique utilisant ce certificat, notamment : - l'indication du début et de la fin de la durée de validité du certificat ; - l'emplacement des services permettant de s'informer du statut de validité du certificat ; - mention indiquant que le certificat est un certificat qualifié de cachet électronique ; - mention indiquant l'utilisation d'un dispositif qualifié de création de cachet électronique ; - la signature électronique avancée ou le cachet électronique avancé du PSCo ; ….
Chapitre II **Section Ière**	**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 validation qualifié de signature/cachet électronique qualifié.

Des prestataires de services de confiance agréés »	**Article 18**	Obligation pour le PSCo agréé 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 validation qualifié de signature/cachet électronique qualifié.

Tableau 2 : *Récapitulatif des principaux articles et dispositions du décret n° 2.22.687 relatifs au service de validation qualifié de signature/cachet électroniques qualifiés.*

5 Procédure d'agrément

Pour un PSCo souhaitant fournir un service de validation qualifié de signature/cachet électronique qualifié.

5.1 Modalités

Le processus d'agrément d'un PSCo pour la fourniture d'un service de validation qualifié de signature et/ou de cachet électronique qualifié est décrit au niveau du référentiel **[Ref_PSCo_Ag]**.

Les critères de conformité et les exigences associées conditionnant l'obtention de l'agrément pour le service de validation qualifié de signature et/ou de cachet électronique qualifié sont précisés plus bas dans le 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 du service de validation qualifié de signature et/ou de cachet électronique qualifié, 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 fournir un service de validation qualifié de signature et de cachet électronique qualifié (articles 11, 20 et 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 validation qualifié) avant l'établissement d'une relation contractuelle avec un futur client/utilisateur (article 33.2.a de la 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 validation qualifié).
(articles 33.2.b et 39 de la loi n°43-20, article 18 du décret 2.22.687) ;

(Critère 6) Garantir que le processus de validation destiné à confirmer la validité d'une signature électronique qualifié, permet de vérifier que :

- Le certificat sur lequel repose la signature était, au moment de la signature, un certificat qualifié de signature électronique ;
- Le certificat qualifié émis par un PSCo agréé était valide au moment de la signature ;
- Les données de validation de la signature correspondent aux données communiquées à la partie utilisatrice ;

- L'ensemble unique de données représentant le signataire dans le certificat est correctement fourni à la partie utilisatrice ;
- L'utilisation d'un pseudonyme est clairement indiquée à la partie utilisatrice, si un pseudonyme a été utilisé au moment de la signature ;
- La signature électronique a été créée par un dispositif qualifié de création de signature électronique et les conditions de création d'une signature avancée ont été satisfaites ;
- L'intégrité des données signées n'a pas été compromise.

(article 10 de la loi n°43-20)

(Critère 7) Garantir que le processus de validation destiné à confirmer la validité d'un cachet électronique qualifié, permet de vérifier que :

- Le certificat sur lequel repose le cachet était, au moment de sa création, un certificat qualifié de cachet électronique ;
- Le certificat qualifié émis par un PSCo agréé était valide au moment de la création du cachet ;
- Les données de validation du cachet correspondent aux données communiquées à la partie utilisatrice ;
- L'ensemble unique de données représentant le créateur du cachet dans le certificat est correctement fourni à la partie utilisatrice ;
- Le cachet électronique a été créé par un dispositif qualifié de création de cachet électronique et les conditions de création d'un cachet avancé ont été satisfaites ;
- L'intégrité des données cachetées n'a pas été compromise.

(article 19 de la loi n°43-20) ;

(Critère 8) Garantir la fourniture du résultat correct du processus de validation aux parties utilisatrices et mettre à leur disposition les moyens de détecter tout problème pertinent relatif à la sécurité du processus de validation (articles 10 et 19 de la loi 43-20) ;

(Critère 9) Garantir la fourniture du résultat du processus de validation aux parties utilisatrices, de manière automatisée, fiable, efficace et portant la signature électronique avancée ou le cachet électronique avancé du prestataire fournissant le service de validation qualifié (articles 11 et 20 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 **validation qualifié de signatures et/ou de cachets électroniques 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 un service de **validation qualifié de signatures et/ou de cachets électroniques qualifiés,** listées **dans le présent document** (chapitre « Exigences de conformité »).

6 Exigences de conformité

Ref_Val_Qual_Exig 1. Le PSCo souhaitant fournir un service de validation qualifié de signature et/ou de cachet électronique qualifié est tenu de prendre connaissance de l'ensemble des documents constituant 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_Val_Qual_Exig 2. Le PSCo souhaitant fournir un service de **validation qualifié de signature et/ou de cachet électronique qualifié** 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 Standards et normes applicables

6.1.1 Standard ETSI TS 119 441

Ref_Val_Qual_Exig 3. Le PSCo, souhaitant fournir un service de validation qualifié de signature et/ou de cachets électroniques qualifiés, est tenu de se conformer aux exigences du standard **ETSI TS 119 441** v1.1.1 ou version ultérieure. Cela comprend :

- Concepts généraux (*chap. 4 – General Concepts*) y inclut :
  - Concepts des exigences de la politique générale *(4.1 General policy requirements concepts) ;*
  - Documentation applicable au service de validation de signatures *(4.2 Signature Validation Service applicable documentation) ;*
  - Composants du service de validation de signatures *(4.3 Signature Validation Service components) ;*
- Evaluation des risques (*chap. 5 – Risk Assessment*) ;
- Politiques et pratiques (*chap. 6 – Policies and practices*) y inclut :
  - Déclaration de pratiques de services de validation de signatures *(6.1 signatures validation service practice statement) ;*
  - Conditions générales *(6.2 Terms and Conditions) ;*
  - Politique en matière de sécurité de l'information *(6.3 Information security policy) ;*
- Gestion et exploitation du service de validation de signatures (*chap. 7 – Signature Validation Service management and operation*) y inclut :
  - Organisation interne *(7.1 Internal organization) ;*
  - Ressources humaines *(7.2 Human ressources) ;*
  - Gestion des actifs *(7.3 Asset management) ;*
  - Contrôle d'accès (7.*4 Access control*) ;
  - Contrôle cryptographiques (7.*5 Cryptographic controls*) ;
  - Sécurité physique et environnementale (7.6 *Physical and environmental security*) ;
  - Sécurité de l'exploitation (7.*7 Operation security*) ;
  - Sécurité réseau *(7.8* Network security*) ;*

- Gestion des incidents *(7.9* Incident management*) ;*
- Collecte de preuves *(7.10 Collection of evidence) ;*
- Gestion de la continuité de service *(7.11* Business continuity management*) ;*
- Cessation d'activité du PSCo et plan associé *(7.12 Signature Validation Service provisioning termination and termination plans) ;*
- Conformité et exigences légales *(7.13 Compliance and legal requirements) ;*

- Exigences techniques du service de validation de signatures (*chap. 8 – Signature validation service technical requirements*) y inclut :
  - Processus de validation de signature *(8.1 Signature validation process) ;*
  - Protocole de validation de signature *(8.2 Signature validation protocol) ;*
  - Interfaces *(8.3 Interfaces) ;*
  - Rapport de validation de signature *(8.4 Signature validation report) ;*
- Cadre pour définition des politiques du service de validation construit sur le présent document (*chap. 9 – Framework for definition of validation service policies built on the present document*) ;
- **Annexe B adressant les spécificités d'un service de validation qualifié signature/cachet électronique qualifié** (Annex B - Qualified Validation Service for QES).

NB : les exigences de la norme ETSI EN 319 102-1 sont applicables mutadis-mutandis au cachet électronique.

La norme ETSI TS 119 441 peut renvoyer vers d'autres normes ou standards (ETSI, ISO/IEC…) 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.

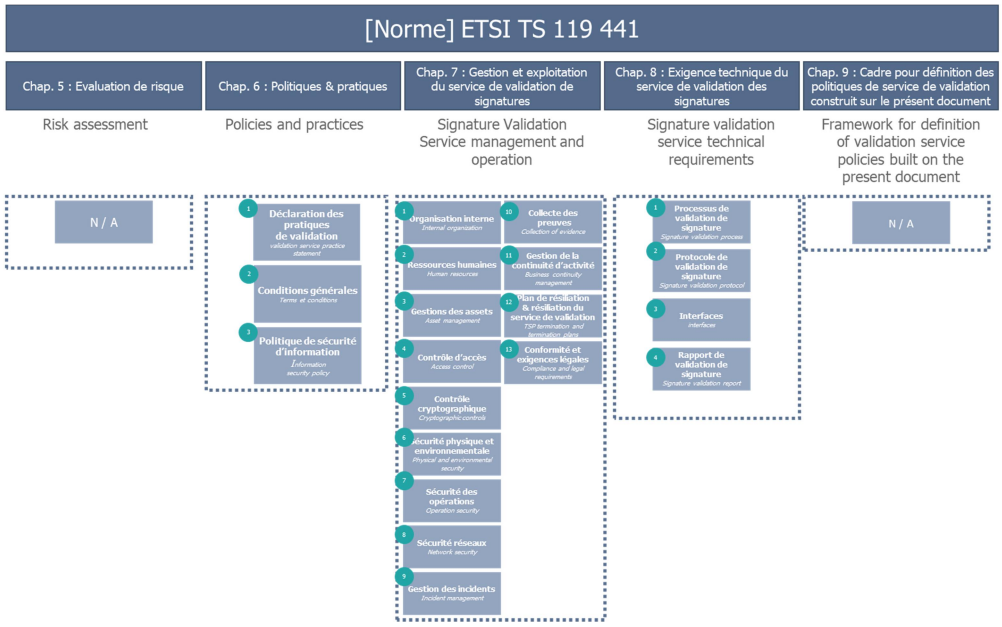

Figure 2 - Sujets couverts par la norme ETSI TS 119 441

NB : les références au standard TS 119-102-1 inclus au niveau de la norme (TS 119 441) peuvent être remplacées par des renvois vers la norme EN 319 102-1.

6.1.2 Norme ETSI EN 319 102-1

Ref_Val_Qual_Exig 4. Le PSCo, souhaitant fournir un service de validation qualifié de signature et/ou de cachets électroniques qualifiés, est tenu de se conformer également aux exigences du **chapitre 5** de la norme **ETSI EN 319 102-1** v1.3.1 ou version ultérieure. Cela comprend :

- Validation de signature *(chap. 5 – signature validation)* y inclut :
  - Modèle de validation de signature *(5.1 Signature validation model) ;*
  - Modules de base *(5.2 Basic building blocks);*
  - Processus de validation des signatures basiques *(5.3 Validation process for Basic Signatures) ;*
  - Module de validation de l'horodatage *(5.4 Time-stamp validation building block);*
  - Processus de validation pour les signatures avec heure et les signatures avec matériel de validation à long terme *(5.5 Validation process for Signatures with Time and Signatures with Long-Term Validation Material) ;*
  - Processus de validation des signatures assurant la disponibilité à long terme et intégrité du matériel de validation *(5.6 Validation process for Signatures providing Long Term Availability and Integrity of Validation Material) ;*
- *Annexe A – Exemples de validation (Annex A - Validation examples).*

NB : les exigences de la norme ETSI EN 319 102-1 sont applicables mutadis-mutandis au cachet électronique.

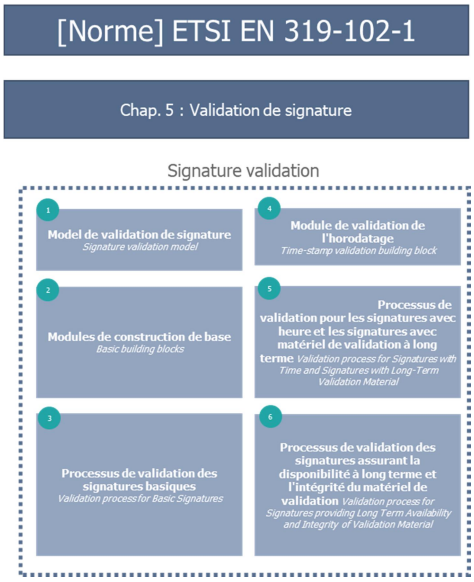

Figure 3 : Sujets couverts par la norme ETSI EN 319 102-1.

6.2 Compléments et précisions

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

- Aux dispositions des normes/standards applicables ETSI TS 119 441 (y compris l'annexe B) et ETSI EN 319 102-1 (chapitre 5 et annexe A) ;
- Aux dispositions des articles applicables de la loi 43-20 et du décret 2.22.687.

6.2.1 Date et heure de référence

Pour se conformer aux dispositions des articles 10 et 19 de la loi 43-20 (et aux critères de conformité 6 et 7), le processus de validation qualifié doit connaître la date et l'heure de création de la signature/ cachet électronique qualifié (date et heure de référence), afin de pouvoir vérifier :

- Que le certificat était bien dans sa période de validité ;
- Que le certificat n'était pas révoqué ;
- Que le PSCo ayant délivré le certificat était bien agréé pour la délivrance de certificats qualifiés.

Ref_Val_Qual_Exig 5. Si la date et l'heure sont associées à la création de la signature/cachet électronique qualifié au travers d'un **horodatage électronique qualifié**, le PSCo du service de validation qualifié :

- Utilise obligatoirement cette date et cette heure comme référence pour le service de validation ;
- Réalise l'ensemble des opérations techniques nécessaires à la validation du jeton d'horodatage qualifié conformément à [Ref_Horo_Qual], dont notamment :
    - Les vérifications des informations relatives à ce service d'horodatage électronique qualifié dans la liste LNPA, conformément aux prescriptions du standard [TS_119_612] (statut qualifié du service, présence du certificat de l'unité d'horodatage électronique ou de l'autorité de certification émettrice dans cette liste) ;
    - Les vérifications relatives à la cryptographie (vérification de l'empreinte et de la signature figurant dans le jeton d'horodatage).

Ref_Val_Qual_Exig 6. Si la date et l'heure ne sont pas associées à la création de la signature/cachet électronique qualifié au travers d'un horodatage électronique, le PSCo agréé du service de validation qualifié utilise comme référence pour le service de validation, la date et l'heure auxquelles la signature/cachet électronique est fourni au service de validation.

Ref_Val_Qual_Exig 7. Si la date et l'heure sont associées à la signature ou au cachet au moyen d'un horodatage électronique non qualifié, il appartient au PSCo agréé du service de validation qualifié d'accepter ou non comme référence de validation cette date et cette heure. En cas de non-acceptation, la date et l'heure de référence sont celles du moment de la validation. Le PSCo agréé doit rendre publique sa politique d'acceptation des horodatages non qualifiés (incluant les modalités de vérification des jetons d'horodatage électronique).

6.2.2 Statut agréé du PSCo ayant délivré le certificat qualifié

Ref_Val_Qual_Exig 8. Le PSCo agréé fournissant le service de validation qualifié doit s'assurer que le prestataire avant délivré le certificat qualifié de signature/cachet objet de la validation, était bien un PSCo agréé pour la délivrance de certificats qualifiés :

- Au **moment de la délivrance** du certificat qualifié ;
- Au **moment de la création de la signature/cachet qualifié** objet de la **validation.**

Ref_Val_Qual_Exig 9. Le PSCo agréé fournissant un service de validation qualifié de signature/cachet électronique qualifié s'appuiera notamment sur la liste nationale des PSCo agréés (LNPA) publiée par l'autorité nationale sur son site internet :

- Vérifier sur la liste LNPA la présence et le statut du PSCo (agréé pour la délivrance de certificats qualifiés) au moment de la délivrance du certificat qualifié ;
- Vérifier sur la liste LNPA la présence et le statut du PSCo (agréé pour la délivrance de certificats qualifiés) au moment de la création de la signature/cachet qualifié objet de la validation ;

- Vérifier que le champ « Service Type Identifier » est valorisé conformément aux spécifications du paragraphe « 5.5.1 Service type identifier » du standard ETSI TS 119 612, pour un PSCo Agréé (prestataire Qualifié au sens de la réglementation EU) ;
- Vérifier que le champ « Service Digital Identifier » est valorisé conformément aux spécifications du paragraphe « 5.5.3 Service digital identifier » du standard ETSI TS 119 612 : le champ doit contenir le certificat d'une Autorité de Certification à partir de laquelle un chemin de validation peut être construit jusqu'au certificat qualifié de signature ou de cachet.

6.2.3 Statut qualifié du certificat

Ref_Val_Qual_Exig 10. Le processus de validation mis en œuvre doit permettre de vérifier que le certificat sur lequel repose la signature/cachet a été, au moment de la signature ou de la création du cachet, un certificat qualifié de signature/cachet électronique. Pour ce faire, le PSCo agréé du service de validation qualifié doit :

- S'assurer que l'extension esi4-qcStatement-1 est valorisée à « **id-etsi-qcs-QcCompliance** » (*Indication que le certificat émis est qualifié)* conformément à [Ref_Deliv_Cert_Qual] ;
- S'assurer que le certificat était bien dans sa **période de validité** au moment de la signature/cachet ;
- S'assurer que le **certificat n'était pas révoqué** au moment de la signature au travers de la CRL ;
- S'assurer que l'extension esi4-qcStatement-6 est valorisée à :
  - "id-etsi-qct-esign" pour un certificat qualifié de signature électronique ;
  - "id-etsi-qct-eseal" pour un certificat qualifié de cachet électronique.

6.2.4 Statut qualifié du dispositif de création de signature/cachet

Ref_Val_Qual_Exig 11. Afin de vérifier que la signature/cachet électronique qualifié a été créée par un dispositif qualifié de création de signature / cachet, le PSCo agréé du service de validation qualifié doit s'assurer que l'extension esi4-qcStatement-4 est valorisée à "id-etsi-qcs-QcSSCD" conformément à [Ref_Deliv_Cert_Qual].

6.2.5 Données du signataire / créateur du cachet

Ref_Val_Qual_Exig 12. Le PSCo agréé du service de validation qualifié doit vérifier que :

- L'ensemble unique des données représentant le signataire (ou le créateur du cachet) dans le certificat est correctement fourni à la partie utilisatrice ;
- Le cas échéant, l'utilisation d'un pseudonyme est clairement indiquée à la partie utilisatrice si un pseudonyme a été utilisé au moment de la signature.

Pour ce faire, le PSCo agréé doit vérifier :

- Que Le champ « Subject » est valorisé conformément au référentiel [Ref_Deliv_Cert_Qual] ;
- La présence au niveau du rapport de validation de l'identité extraite du champ « Subject » ainsi qu'une mention relative à l'utilisation d'un pseudonyme le cas échéant.

6.2.6 Informations de révocation

Ref_Val_Qual_Exig 13. Le service de validation doit systématiquement solliciter les informations les plus récentes mises à disposition par l'autorité de certification émettrice du certificat qualifié sur lequel repose la signature/cachet électronique objet de la validation.

Ref_Val_Qual_Exig 14. Si cette autorité de certification émettrice met à disposition un service de répondeur OCSP, le PSCo agréé s'appuiera sur celui-ci comme source pour les informations de révocation.

6.2.7 Intégrité des données signées/cachetés

Ref_Val_Qual_Exig 15. Conformément aux articles 10 et 19, le service de validation doit vérifier que l'intégrité des données signées/cachetées n'a pas été compromise. Pour ce faire la clause 5.2.7 de la norme EN 319 102 -1 s'applique. Le PSCo agréé doit en complément s'assurer que les algorithmes et mécanismes cryptographiques utilisés respectent les spécifications indiquées au niveau du référentiel [Ref_PSCo_Ag].

6.2.8 Protection de l'application de validation

Ref_Val_Qual_Exig 16. Le PSCo agréé doit mettre en place des mesures techniques et organisationnelles appropriées afin d'assurer la sécurité de l'application utilisée pour réaliser la validation qualifiée des signatures/cachets électroniques qualifiés. Cette application doit à minima être alignée avec les prérogatives Common Criteria EAL2 ou équivalent (équivalence validée par l'autorité) ; la certification Common Criteria EAL2 est recommandée.

6.2.9 Résultat de la validation

Ref_Val_Qual_Exig 17. Le résultat du processus de validation devra être fourni via :

- Un **statut** de la validation ;
- **Un rapport simple** de synthèse reprenant le statut et les principales décisions ;
- Un **rapport de validation détaillé** permettant l'étude détaillée des décisions prises durant la phase de validation et la justification du statut de validation ;
- Ces rapports doivent être réalisés conformément aux exigences au standard ETSI TS 119 441 en particulier la clause 8.4 et les spécifications Annexe B.

Ref_Val_Qual_Exig 18. Les rapports de validation (simple et détaillé) et l'indication du statut doivent être mis à disposition de la partie utilisatrice, de manière automatisée, fiable et efficace.

Ref_Val_Qual_Exig 19. Les rapports de validation (simple et détaillé) doivent porter la **signature électronique avancée** ou le **cachet électronique avancé** du PSCo agréé fournissant le service de validation qualifié.

Ref_Val_Qual_Exig 20. Le PSCo agréé fournissant le service de validation qualifié est tenu de rendre publique sa politique de validation des signatures électroniques qualifiées ou des cachets électroniques qualifiés afin de permettre la bonne interprétation du rapport de validation.

6.2.10 Cessation d'activité

Ref_Val_Qual_Exig 21. En cas de cessation d'activité, le PSCo agréé du service de validation qualifié, doit détruire les clés privées utilisées pour signer (ou cacheter) les rapports de validation.

6.2.11 Conservation des données

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

En complément aux indications du référentiel [Ref_PSCo_AG] et aux exigences de la clause 7.10 du standard TS 119 441.

Ref_Val_Qual_Exig 22. Conformément à l'article 18 du décret n° 2.22.687, le PSCo agréé du service de validation qualifié est tenu de conserver pendant une **durée minimale de sept (7) ans**, toutes les informations pertinentes concernant les données délivrées et reçues dans le cadre de la fourniture du service de validation, notamment afin de pouvoir assurer le service et le cas échéant fournir des preuves suffisantes en cas de litige.

Ref_Val_Qual_Exig 23. En complément des données précisées à la clause 7.10 « Collection of Evidence « de la norme TS 119 441 V1.1.1, le PSCo agréé du service de validation qualifié est tenu de conserver a minima :

- Les **données fournies par le demandeur** pour la validation de signature ou de cachet électronique (y compris la valeur de la signature électronique ou du cachet électronique si est séparable du document signé/cacheté ou représentation unique du document signé dans le cas contraire) ;
- **Identité du demandeur** si celui-ci a fait l'objet d'une identification pour l'accès au service ;
- La **date et l'heure de la validation** de la signature ou du cachet électronique qualifié ;
- Les **données externes** utilisées pour valider la signature ou le *cachet (exemple : listes de confiance, listes CRL, réponses OCSP, …) ;*
- Les **rapports de validation** (simples et détaillés) contenant le résultat de la validation qualifiée de la signature ou du cachet électronique qualifié ;
- Toute autre donnée jugée pertinente dans la fourniture dudit service.

6.2.12 Modules cryptographiques utilisés

Ref_Val_Qual_Exig 24. Les modules cryptographiques utilisés pour apposer la signature électronique avancée ou le cachet électronique avancé du PSCo agréé sur le rapport de validation de signature/cachet électronique qualifié, doivent être conformes aux exigences relatives aux modules cryptographiques utilisés par les PSCo agréés spécifiés au niveau du référentiel [Ref_PSCo_Ag].

6.2.13 Publication sur la liste nationale des PSCo agréés

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

Ref_Val_Qual_Exig 25. L'identification d'un service de validation qualifié de signature et/ou de cachet électronique qualifié dans la Liste Nationale des PSCo Agréés (LNPA) doit respecter les exigences définies dans [Ref_PSCo_AG].

Ref_Val_Qual_Exig 26. L'identification d'un service de validation qualifié de signature et/ou de cachet électronique qualifié, dans la Liste Nationale des PSCo Agréés (LNPA) se fait :

- Soit au moyen du certificat électronique utilisé par le PSCo agréé pour apposer un cachet (ou une signature) sur le rapport de validation :
    - Dans ce cas, si plusieurs certificats de cachet électronique (ou de signature) sont mis en œuvre pour un même service de conservation qualifié, cela donne lieu à l'inscription de plusieurs services dans la liste de confiance ;
- Soit au moyen du certificat électronique d'une autorité de certification (AC) opérée sous la responsabilité du PSCo agréé et qui satisfait les 2 conditions suivantes :

(1) L'AC ne délivre des certificats qu'à l'attention exclusive de services de confiance opérés par le PSCo agréé ;

(2) L'AC ne délivre pas de certificats pour des services de validation non qualifiés (autrement dit, aucun service de validation non qualifié ne fait pas partie des services de confiance opérés par le PSCo agréé sous l'AC en question) :

- Dans ce cas, le PSCo doit pouvoir démontrer le respect des conditions (1) et (2) et la mise en place de mesures organisationnelles et techniques appropriées afin d'assurer le maintien du respect de ces 2 conditions dans la durée ;

- Soit par le biais d'un autre élément d'identification représentant le service sans ambiguïté dans le respect des exigences de la clause 5.5.3 du standard [TS_119_612] :
  - Le PSCo agréé justifiera de la pertinence de son choix pour l'identification du service.

7 Annexes

Liens vers les normes et standard

- **ETSI TS_119_441 :** Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services.
  - Se référer à la version la plus récente publiée sur le site de l'ETSI **:**

    https://www.etsi.org/deliver/etsi_ts/119400_119499/119441/01.01.01_60/ts_119441v010101p.pdf
  - 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_119499/119441/

- **ETSI EN_319_102-1 :** Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation – **Clause 5 « Signature validation »** ainsi que **« l'Annexe A »**.
  - **Se référer à la version la plus récente** publiée sur le site de l'ETSI :

    https://www.etsi.org/deliver/etsi_en/319100_319199/31910201/01.03.01_60/en_31910201v010301p.pdf
  - 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/319100_319199/31910201/

- **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