



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

6

[Ref_Conserv_Qual]

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



Suivi des mises à jour du document [Ref_Conserv_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	4
2	Objet et périmètre	5
3	Modalités de mise à jour	6
4	Cadre de référence	7
4.1	Cadre juridique et normatif	7
4.2	Précaution d'interprétation des normes et standards ETSI	8
4.3	Rappel des principales dispositions de la loi n°43-20 applicables	8
4.4	Rappel des principales dispositions du décret n° 2.22.687 applicables	9
5	Procédure d'agrément	10
5.1	Modalités	10
5.2	Critères de conformité	10
6	Exigences de conformité	12
6.1	Normes et standards applicables	12
6.1.1	Cas de l'approche (1) spécifique unitaire	12
6.1.2	Cas de l'approche alternative (2) SAE	14
6.2	Compléments et précisions	14
6.2.1	Accusé de réception	15
6.2.2	Données signées/cachetées	15
6.2.3	Réversibilité et restitution des données	15
6.2.4	Validation et scellement	16
6.2.5	Formats de signature/cachets conservés	17
6.2.6	Conservation des données	17
6.2.7	Modules cryptographiques utilisés	18
6.2.8	Publication sur la liste nationale des PSCo agréés	18
7	Annexes	19
7.1.1	Liens vers les normes et standard	19

1 Terminologie et acronymes

AC : autorité de certification en charge de créer et d'attribuer les certificats.

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).

Liste nationale des PSCo agréés (LNPA) par l'autorité nationale : désigne, conformément à l'article 53 de la Loi n°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.

Métadonnées : ensemble structuré de données techniques relatives à un document, servant à décrire les caractéristiques de ce document en vue de faciliter son indexation, sa consultation, son usage ou sa conservation.

PA : Politique d'archivage électronique.

PC : Politique de Certification.

PSCo : prestataire de service de confiance au sens de la Loi n° 43-20. Dans ce document, le terme PSCo désigne également un prestataire souhaitant devenir PSCo.

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.

SAE (Système d'Archivage Electronique) : système permettant de recevoir, conserver, traiter, restituer des archives électroniques.

WOS (Preservation service WithOut STorage) : modèle de conservation sans stockage des données conformément au standard TS 119 511.

WTS (Preservation service With Temporary Storage) : modèle de conservation avec stockage temporaire des données conformément au standard TS 119 511.

WST (Preservation service With STorage) : modèle de conservation avec stockage des données conformément au standard TS 119 511.

2 Objet et périmètre

Le présent document, désigné par **[Ref_Conserv_Qual]**, constitue le référentiel fixant les exigences de conformité à respecter par les PSCo fournissant un **service de conservation qualifié de signature et/ou de cachet électronique qualifié** et ce conformément au **cadre légal national** rappelé dans le présent document au chapitre « Cadre légal de référence ».

Le respect des exigences des référentiels [Ref_Conserv_Qual] & [Ref_PSCo_AG] conditionnent l'obtention de l'agrément pour la fourniture des services de conservation qualifiés de signatures et/ou de cachets 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 n° 43-20).

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

3 Modalités de mise à jour

L'autorité nationale veille à ce que le référentiel d'exigences reste en cohérence avec le cadre réglementaire national 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_Conserv_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 jourada I 1442 (31 décembre 2020) :
 - Les principales dispositions spécifiques de la loi n°43-20 sont rappelées au niveau du chapitre **Erreur ! Source du renvoi introuvable.** 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_Conserv_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] ETSI TS_119_511 v1.1.1** ou version ultérieure : Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques.

Définit les exigences normatives relatives aux prestataires de services de confiance fournissant un service de conservation de signatures et/ou de cachets électroniques.

- **[Norme] ISO 14641-1**: Electronic document management — Design and operation of an information system for the preservation of electronic documents — Specifications.

Archivage électronique - Conception et exploitation d'un système informatique pour la conservation intègre de documents électroniques.

- **[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.

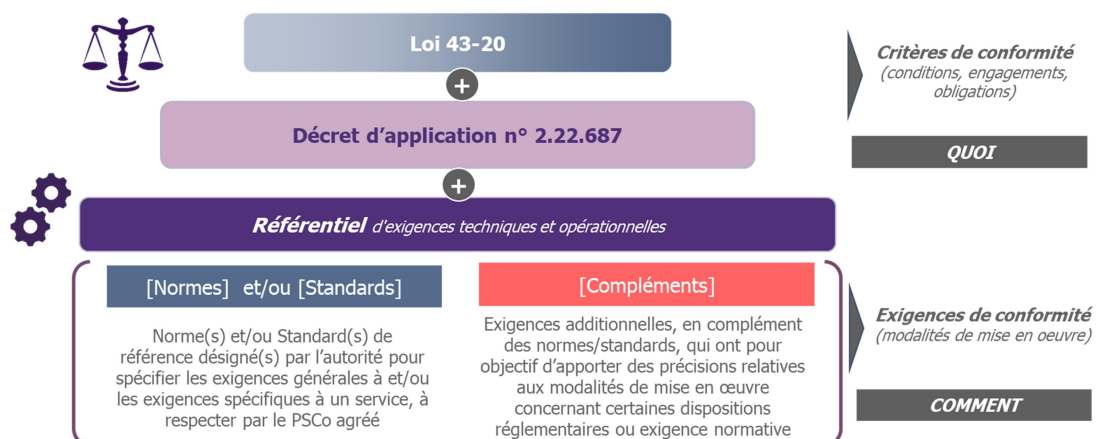


Figure 1 - Structure du cadre juridique et normatif

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 « **shall / 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 conservation qualifié de signature et/ou de cachet électronique qualifié sont consolidés au niveau du tableau suivant :

Chapitre Ier Section Ière <i>Des services de confiance</i> Sous-sections 1&2	Article 12	Seul un <u>PCSo agréé</u> utilisant des <u>procédures et technologies</u> permettant <u>d'étendre la fiabilité</u> des signatures électroniques <u>au-delà de la période de validité technologique</u> peut fournir un service de <u>conservation qualifié de signatures électroniques qualifiées</u> .
	Article 21	Seul un <u>PCSo agréé</u> utilisant des <u>procédures et technologies</u> permettant <u>d'étendre la fiabilité</u> des cachets électroniques <u>au-delà de la période de validité technologique</u> peut fournir un service de conservation qualifié de cachets électroniques qualifiés.
Chapitre Ier Section II <i>Des prestataires de services de confiance</i>	Article 32	Obligation d'agrément : seuls les PSCo agréés peuvent fournir un service* de confiance qualifié et gérer les opérations y afférentes. * ici service de conservation qualifié de signature/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 le service de conservation qualifié de signature/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 le service de conservation qualifié de signature/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 le service de conservation qualifié de signature/cachet électronique qualifié.

Tableau 1 : Récapitulatif des principaux articles et dispositions de la loi 43-20 relatifs au service de conservation qualifié de signature/cachet électronique qualifié

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 conservation qualifié de signature et/ou de cachet électronique qualifié, sont consolidés au niveau du tableau suivant :

Chapitre II Section Ière <i>Des prestataires de services de confiance agréés</i>	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 le service de conservation qualifié de signature/cachet électronique qualifié.
	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 le service de conservation qualifié de signature/cachet électronique qualifié.

Tableau 2 : Récapitulatif des principaux articles et dispositions du décret n° 2.22.687 relatifs au service de conservation qualifié de signature/cachet électronique qualifié

5 Procédure d'agrément

Pour un PSCo agréé fournissant un service de conservation qualifié de signature et/ou de cachet électronique qualifié.

5.1 Modalités

Le processus d'agrément d'un PSCo pour la fourniture d'un service de conservation qualifié de signature et/ou de cachet électronique qualifié doit être conforme au processus d'agrément tel que décrit au niveau du référentiel [Ref_PSCo_AG].

Les critères de conformité et les exigences associées conditionnant l'obtention de l'agrément pour la fourniture d'un service de conservation 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 de fournir un service de conservation 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 conservation de signature et/ou de cachet électronique qualifié (articles 12, 21 et 32 de la loi n°43-20) ;
- (Critère 2) Utiliser des procédures et des technologies permettant de garantir l'extension de la fiabilité des signatures électroniques au-delà de la validité technologique (article 12 de la loi n°43-20) ;
- (Critère 3) Utiliser des procédures et des technologies permettant de garantir l'extension de la fiabilité des cachets électroniques au-delà de la validité technologique (article 21 de la loi n°43-20) ;
- (Critère 4) Utiliser des systèmes, matériels et logiciels fiables et assurer leur sécurité technique (article 33 de la loi n°43-20) ;
- (Critère 5) Assurer la fiabilité des processus mis en œuvre (article 33 de la loi n°43-20) ;
- (Critère 6) Préciser de façon exhaustive les conditions et limites d'utilisation du service de confiance qualifié (ici service de conservation qualifié) avant l'établissement d'une relation contractuelle avec un futur client/utilisateur (article 33.2.a de loi n°43-20) ;
- (Critère 7) 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 horodatage qualifié) (articles 33.2.b et 39 de loi n°43-20, article 18 du décret 2.22.687) ;

A noter :

Le respect de ces **critères de conformité** se matérialise par la **mise en œuvre** de la part du PSCo souhaitant offrir un service **de conservation qualifié de signature/cachet électronique qualifié**, 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 conservation qualifié de signature et/ou de cachet électronique qualifié** listées plus bas dans le présent document (chapitre « Exigences de conformité ») selon l'approche de conservation adoptée.

6 Exigences de conformité

2 approches sont admises pour fournir le service de conservation qualifié de signature/cachet électronique qualifié :

(1) Approche spécifique unitaire par signature/cachet électronique (extension de la fiabilité unitairement)

Conformément au standard **ETSI TS 119 511**, l'approche de conservation spécifique unitaire se décline en 3 variantes, toutes admises pour étendre la fiabilité « unitaire » d'une signature (ou d'un cachet) électronique qualifiée (qualifié) au-delà de la période de validité technologique (articles 12 et 21 Loi 43-20) et assurer ainsi la conservation qualifiée de ladite signature (ou dudit cachet)

1. Variante avec stockage (*Preservation service With Storage – WST*) ;

2. Variante sans stockage (*Preservation service WithOut Storage – WOS*) ;

3. Variante avec stockage temporaire (*Preservation service With Temporary Storage – WTS*).

[Pour les définitions, se référer au paragraphe 4.1 du standard ETSI TS 119 511]

(2) Approche alternative systémique SAE (fiabilisation du contenant)

Outre l'approche spécifique et ses variantes, une **approche alternative** plus globale, reposant sur la protection en intégrité d'un **Système d'Archivage Electronique (SAE)** dans lequel seront conservés les signatures et cachets électroniques qualifiés, peut également être admise pour fournir un service de conservation qualifié à condition que le SAE utilisé soit conforme aux exigences précisées dans ce chapitre « exigences de conformité ».

Ref_Conserv_Qual 1. Le PSCo souhaitant fournir un service de conservation qualifié des 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'un des standards (ou normes) applicables indiqués, et d'autre part une disposition précise de la loi n°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 procéder éventuellement à une rectification.

Ref_Conserv_Qual 2. Le PSCo souhaitant fournir un service de conservation qualifié de signature et/ou de cachet électronique qualifié doit être agréé au sens de la loi n°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 et standards applicables

6.1.1 Cas de l'approche (1) spécifique unitaire

Ref_Conserv_Qual 3. Le PSCo souhaitant fournir un service de **conservation qualifié des signature/cachet électronique qualifié** en se basant pas sur l'approche (1) spécifique unitaire (extension de la fiabilité de la signature ou du cachet qualifié) est tenu de respecter les exigences de la norme **ETSI TS 119 511** (v1.1.1 ou version ultérieure). Cela comprend :

- Concepts généraux (*chap. 4 – General Concepts*) y inclut :
 - Modèles de stockage (*4.1 Preservation storage models*) ;
 - Objectifs fonctionnels (*4.2 Functional goals*) ;

- Documentation applicable au service de conservation (4.3 *Preservation service applicable documentation*) ;
- Durée de validité des preuves (4.4 *Expected evidence duration*) ;
- Période de conservation (4.5 *Preservation period*) ;
- Evaluation des risques (chap. 5 – *Risk Assessment*) ;
- Politiques et pratiques (chap. 6 – *Policies and practices*) y inclut :
 - Déclaration des pratiques d'un service de conservation (6.1 *Preservation service practice statement*) ;
 - Conditions générales (6.2 *Terms and Conditions*) ;
 - Politique en matière de sécurité de l'information (6.3 *Information security policy*) ;
 - Conservation de profils (6.4 *Preservation profiles*) ;
 - Politique de conservation des preuves (6.5 *Preservation evidence policy*) ;
 - Politique de validation des signatures (6.6 *Signature validation policy*) ;
 - Consentement d'abonnement (6.7 *Subscriber agreement*) ;
- Management et exploitation des fournisseurs de services de conservation (chap. 7 – *PSP management and operation*) y inclut :
 - Organisation interne (7.1 *Internal organization*) ;
 - Ressources humaines (7.2 *Human resources*) ;
 - 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 *TSP termination and termination plans*) ;
 - Conformité (7.13 *Compliance*) ;
 - Supervision de la cryptographie (7.14 *Cryptographic monitoring*) ;
 - Prolongement de la durée de conservation des preuves (7.15 *Augmentation of preservation evidences*) ;
 - Export-import package (7.16 *Export-import package*) ;
- Protocoles d'exploitation et de notification (chap. 8 – *Operational and notification protocols*) y inclut :
 - Protocole de conservation (8.1 *Preservation protocol*) ;
 - Protocole de notification (8.2 *Notification protocol*) ;
- Procédures de conservation (chap. 9 – *Preservation process*) y inclut :
 - Stockage des données/preuves conservées (9.1 *Storage of preserved data and evidences*) ;

- Conservation des preuves (9.2 Preservation evidences) ;
- Conservation des signatures électroniques (9.3 Preservation of digital signatures) ;
- Les Annexes notamment **l'Annexe A précisant des exigences spécifiques relatives au service de conservation qualifié.**

Le standard ETSI TS 119 511 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.

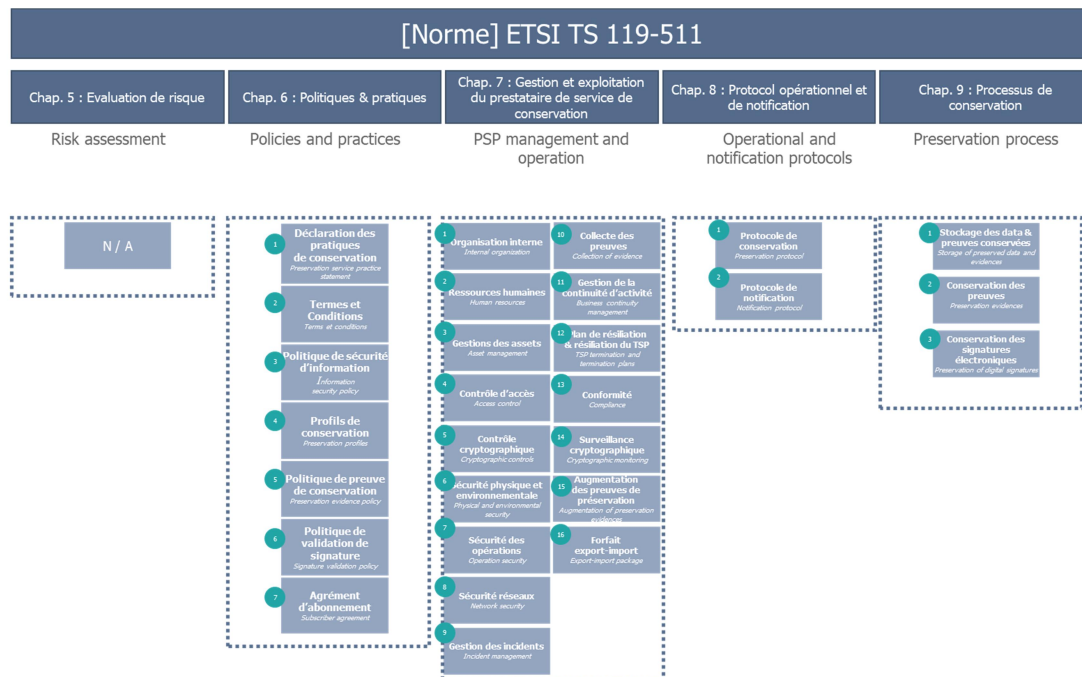


Figure 2- Sujets couverts par la norme ETSI TS 119 511

6.1.2 Cas de l'approche alternative (2) SAE

Ref_Conserv_ Qual 4. Le PSCo souhaitant fournir un service de **conservation qualifié des signature/cachet électronique qualifié** en se basant sur un système d'archivage électronique est tenu de respecter les exigences de la norme **[ISO 14641-1]** pour assurer la pérennité, l'intégrité, la sécurité et la traçabilité :

- **[ISO 14641-1] Archivage électronique — Conception et exploitation d'un système informatique pour la conservation intégrée de documents électroniques ;**

L'appui sur les normes ci-dessous est recommandé :

- [ISO 14721] concernant la conservation à long terme quelles que soient les évolutions technologiques ;
- [ISO 16363] concernant la sécurisation des systèmes de transfert des informations.

6.2 Compléments et précisions

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

- Aux dispositions des normes/standards applicables ;
- Aux dispositions des articles applicables de la loi 43-20 et du décret 2.22.687.

Sauf mention spécifique contraire, ces exigences complémentaires s'appliquent aux différentes approches de conservation.

6.2.1 Accusé de réception

Recommandation : il est recommandé que le PSCo transmette un accusé de réception, cacheté et/ou horodaté, relatif à la demande de conservation lors du dépôt d'une signature ou d'un cachet électronique qualifié auprès du service de conservation par un demandeur.

6.2.2 Données signées/cachetées

Ref_Conserv_Qual 5. Le PSCo agréé doit s'assurer que la conservation du document (ou des données) objet de la signature/cachet électronique qualifié conservé(e), est réalisée, par ledit PSCo ou par un tiers, dans les meilleures conditions de protection en intégrité, notamment pour pallier au risque d'affaiblissement de la fonction de calcul d'empreinte liant le document et la signature ou le cachet.

Il est recommandé que le document signé/cacheté (dont la signature/cachet fait l'objet de la conservation qualifiée) soit directement conservé et pas uniquement son empreinte (hash) signée/cachetée.

6.2.3 Réversibilité et restitution des données

La réversibilité est la faculté d'extraction (récupération) d'un système de conservation de tout ou partie des éléments qui y sont conservés ainsi qu'éventuellement toutes les métadonnées associées.

La réversibilité permet notamment d'éviter la dépendance par rapport à un système en permettant de migrer l'ensemble des documents d'un système vers un autre.

Ref_Conserv_Qual 6. Le PSCo agréé fournissant un service de conservation qualifié de signatures et/ou de cachets électroniques doit :

- Garantir la réversibilité de l'ensemble des éléments conservés ;
- Garantir l'intégrité et l'exploitabilité de l'ensemble des éléments reversés.

Ref_Conserv_Qual 7. La réversibilité des contenus signés/cachetés ne consiste pas simplement à restituer les données signées/cachetées. Le PSCo agréé doit s'assurer que les modalités de réversibilité mises en place permettent de récupérer tous les éléments nécessaires au maintien de la vocation probatoire et de la traçabilité.

Ref_Conserv_Qual 8. La fiabilité des signatures et cachets électroniques qualifiés conservés ne doit pas être affectée par cette réversibilité.

Ref_Conserv_Qual 9. Si les éléments reversés sont dans un format non standard, le PSCo agréé doit :

- Mettre à disposition du destinataire les spécifications associés et si nécessaire les outils permettant leur lecture ;
- Ou, transférer ces éléments à un format standard pérenne et lisible.

Ref_Conserv_Qual 10. Si les éléments reversés sont protégés par un jeton horodatage ou un cachet électronique, les informations (CRL, PC...) relatives aux *certificats électroniques* utilisées doivent être accessibles de sorte que la validation de ces services (horodatage, cachet) soit réalisable par le destinataire de la réversibilité (*usage par exemple du certificat électronique identifiant le service dans la liste de confiance*).

6.2.4 Validation et scellement

Quelle que soit l'approche de conservation

Ref_Conserv_Qual 11. Les services mis en œuvre pour la validation qualifiée de signature/cachet électronique qualifié doivent obligatoirement être conformes aux exigences du référentiel [Ref_Valid_Qual].

Ref_Conserv_Qual 12. La politique de validation à appliquer dans le cadre du service de conservation, doit être préalablement établie.

Cas de l'approche SAE

Ref_Conserv_Qual 13. Dans le cas de **l'approche (2), conservation sur la base d'un SAE**, une **validation qualifiée** de la signature/cachet électronique qualifié objet du service de conservation doit **obligatoirement** être mise en œuvre **préalablement à son archivage électronique**. Le résultat de la validation doit être archivé avec la signature ou le cachet électronique qualifié à conserver.

Ref_Conserv_Qual 14. Le PSCo agréé fournissant le service de conservation qualifié pourra s'appuyer sur un **PSCo agréé tiers** pour réaliser la validation qualifiée. Dans ce cas :

- La signature/cachet apposé par le PSCo agréé fournissant le service de validation qualifié sur le rapport de validation **doit être vérifié avant de procéder à l'archivage de la signature/cachet électronique qualifié** ;
- La **validation** doit être également **archivée**.

Ref_Conserv_Qual 15. Lorsque la validation est concluante, la réponse du service de validation (comprenant les rapports de de validation signés ou cachetés) est directement rajoutée à l'archive, auprès du document comprenant la signature/cachet électronique. Le PSCo agréé réalise le scellement de chaque dossier d'archive à l'aide, a minima, d'un cachet électronique avancé avec horodatage, apposé de manière à englober les 4 constituants de l'archive à savoir :

- Le document archivé (document signé ou cacheté) ;
- Les métadonnées associées ;
- Les rapports de validation ;
- Les métadonnées de gestion.

Ref_Conserv_Qual 16. Le PSCo agréé doit a minima de nouveau sceller l'archive dans les cas suivants :

- Modification de la durée de conservation ;
- Modification des métadonnées associées au document ;
- Modification des métadonnées administratives ;
- Expiration du certificat utilisé pour le cachet initial ;
- Obsolescence des outils cryptographiques utilisés pour le scellement initial.

Ce nouveau scellement doit s'appuyer a minima sur un nouveau cachet électronique avancé avec horodatage et doit englober l'ensemble des éléments de l'archive y compris le scellement précédent. Le certificat utilisé pour apposer le nouveau cachet doit être choisi, comme pour le dépôt initial, en fonction de la durée de vie restante de l'archive dans le SAE. Ce procédé de sur-scellement devra être appliqué autant de fois que nécessaire au cours de la vie d'une archive.

Ref_Conserv_ Qual 17. Lorsque le PSCo agréé a recours à des supports réinscriptibles ou à des supports de type WORM logiques, les enregistrements doivent faire l'objet d'un horodatage électronique régulier, à une périodicité définie en fonction des résultats de l'analyse des risques et de l'état de l'art de la cryptographie. Il est recommandé que cet horodatage électronique soit qualifié.

6.2.5 Formats de signature/cachets conservés

Ref_Conserv_ Qual 18. La signature électronique qualifiée (ou le cachet électronique qualifié), à conserver dans le cadre de la fourniture du service de conservation qualifié doit respecter les formats de signature (ou cachet) autorisés précisés au niveau du référentiel [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 de signature (ou cachet) électronique :

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

6.2.6 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 des standards / normes applicables au service de conservation qualifié (ETSI TS 119 511 & ISO 14641-1).

Ref_Conserv_ Qual 19. Le PSCo agréé de service de conservation qualifié de signatures et/ou de cachets électroniques qualifiés doit conserver pendant une durée au moins égale à la durée de conservation des signatures ou cachets électroniques qualifiés, toutes les informations pertinentes concernant les données délivrées et reçues, notamment afin de pouvoir assurer le service et le cas échéant fournir des preuves suffisantes en cas de litige. Cela inclut :

- Le Document signé, dans un format standard (exemple PDF) ou son empreinte (hash) ;
- Des éventuelles métadonnées associées au document (en particulier dans le cas du SAE) ;
- La signature électronique qualifiée (ou le cachet électronique qualifié) objet de la conservation, présentée séparément ou encapsulé dans le document signé/cacheté ;
- Les éléments de preuves (comme la pièce d'identité utilisée), pour garantir l'identité des signataires (ou créateurs du cachet) et l'intégrité des preuves au cours du temps ;
- La validation qualifiée / le rapport de validation.

En complément :

- Les dossiers de souscription (enregistrement) au service de conservation qualifié comportant une formalisation de l'engagement signé (contrat de service, demande de souscription...) ;
- Les Conditions générales d'utilisation du service ;
- La Politique de conservation (ou politique d'archivage électronique le cas échéant) et les politiques des autres services de confiance intervenant dans la fourniture du service (politique d'horodatage, politique de validation, politique de certification, politique de signature...) et les Déclarations de politiques associées ;
- Les jetons d'horodatage électronique qualifiés utilisés ;
- Les journaux (logs) des événements/opérations du service.

Ref_Conserv_ Qual 20. Le PSCo agréé de service de conservation qualifié de signatures et/ou de cachets électroniques qualifiés précise dans ses conditions générales d'utilisation, le cas échéant, la durée supplémentaire effectivement appliquée pour la conservation des preuves (au-delà de la durée

de conservation des signatures et cachets électroniques qualifiés) ainsi que les modalités de réversibilité.

6.2.7 Modules cryptographiques utilisés

Ref_Conserv_Qual 21. Les modules cryptographiques utilisés pour réaliser les opérations nécessaires au service de conservation qualifié de signatures et/ou de cachets électroniques qualifiés, notamment les opérations de création de signature/cachet électronique et les opérations d'horodatage doivent impérativement être conformes aux dispositions relatives aux modules cryptographiques spécifiées au niveau du référentiel [Ref_PSCo_AG].

6.2.8 Publication sur la liste nationale des PSCo agréés

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

Ref_Conserv_Qual 22. L'identification d'un service de conservation 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_Conserv_Qual 23. L'identification d'un service de conservation 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 pour apposer un cachet ou un horodatage sur l'accusé de réception de la demande de conservation :
 - Dans ce cas, si plusieurs certificats de cachet électronique 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 conservation non qualifiés (autrement dit, aucun service de conservation non qualifié ne fait 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

7.1.1 Liens vers les normes et standards

- **Standard ETSI TS 119 511** : Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques,
 - **se référer à la version la plus récente publiée sur le site de l'ETSI :**
https://www.etsi.org/deliver/etsi_ts/119500_119599/119511/
 - à 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/119500_119599/119511/01.01.01_60/ts_119511v010101p.pdf
- **Norme ISO 14641-1** : Electronic document management — Design and operation of an information system for the preservation of electronic documents — Specifications
 - <https://www.iso.org/standard/74338.html>
- **[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%20BJRmarking.pdf