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

1

[Ref_PSCo_AG]

Exigences générales de conformité des prestataires fournissant des services de confiance qualifiés

Suivi des mises à jour du document [Ref_PSCo_AG]

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

Autorité Nationale ou Autorité : fait référence dans 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).

HTR : Horloge Temps Réel.

http : hypertext transfer protocol.

ITILv4 : Information Technology Infrastructure Library version 4.

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.

NTP : Network Time Protocol.

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

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

PSCo sans agrément : désigne un PSCo qui fournit un ou plusieurs services de confiance non qualifiés conformément à la Loi n° 43-20.

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_PSCo_AG]**, constitue **le socle** de référence fixant les exigences générales de conformité à respecter par les **PSCo agrées quel que soit le service de confiance qualifié fourni**, et ce conformément au cadre légal national rappelé dans le présent document notamment au niveau du chapitre « cadre de référence ».

Le respect des exigences [Ref_PSCo_AG] conditionne l'obtention de l'agréement

L'évaluation du respect des exigences [Ref_PSCo_AG] 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)

[Ref_PSCo_AG] est complété par des référentiels dédiés spécifiques [Ref_x] applicables selon la nature du service de confiance qualifié : délivrance de certificats qualifiés, conservation qualifiée de signatures qualifiées et/ou de cachets électroniques qualifiés, envoi recommandé qualifiés, validation de signatures qualifiées et/ou de cachets électroniques qualifiés et horodatage qualifié.

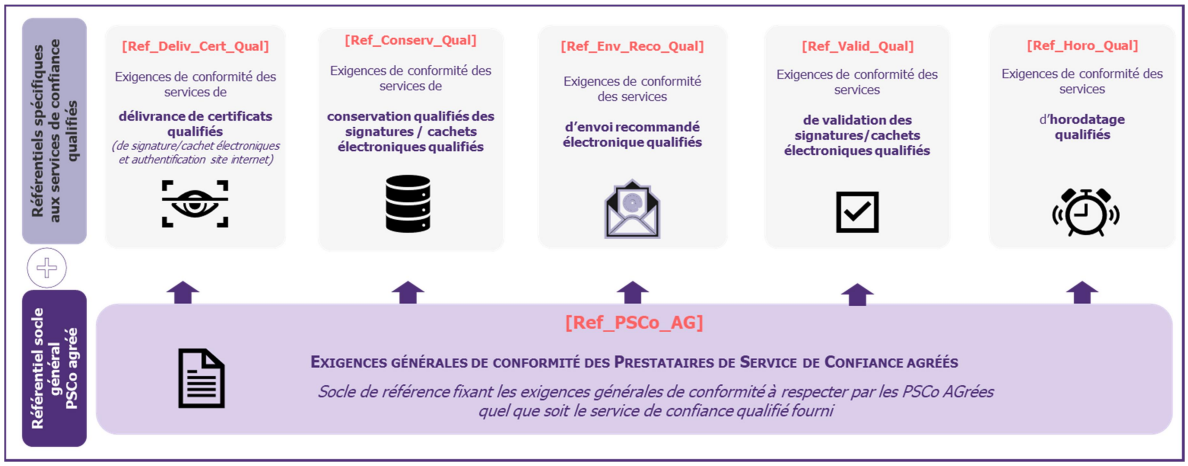

Figure 1 : Structure des référentiels d'exigences.

Liste des référentiels spécifiques aux services de confiance qualifiés

[Ref_Deliv_Cert_Qual] : Exigences de conformité des services de délivrance de certificats qualifiés de signature électronique, de cachet électronique ou d'authentification de site internet.

[Ref_Horo_Qual] : Exigences de conformité des services d'horodatage électronique qualifié.

[Ref_Env_Reco_Qual] : Exigences de conformité des services d'envoi recommandé électronique qualifié.

[Ref_Valid_Qual] : Exigences de conformité des services de validation qualifiés de signatures électroniques qualifiées et/ou de cachets électroniques qualifiés.

[Ref_Conserv_Qual] : Exigences de conformité des services de conservation qualifiés de signatures électroniques qualifiées et/ou de cachets électroniques qualifiés.

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 mises 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_PSCo_AG]** 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_PSCo_AG]** 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 319 401** V2.3.1 (2021-05) ou version ultérieure : Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers ;

  Définit les exigences normatives de politique générale relatives aux Prestataires de Services de Confiance : les pratiques d'organisation, de fonctionnement et de gestion des PSCo ;

  La norme ETSI EN 319 401 peut renvoyer vers d'autres normes (ETSI, ISO, …) afin de spécifier des orientations de mise en œuvre pour certaines exigences ;
- **[Standard] ETSI TS 119 612** V2.2.1 (2016-04) ou version ultérieure : Electronic Signatures and Infrastructures (ESI); Trusted Lists ;

  Définit les exigences normatives à respecter pour l'inscription et l'identification d'un service de confiance dans la liste de confiance nationale publiée et maintenue par l'autorité nationale ;
- **[Standard] ETSI TS 119 312 :** Electronic Signatures and Infrastructures (ESI); Cryptographic Suites ;

  Définit les exigences normatives à respecter pour les algorithmes et mécanismes cryptographiques mis en œuvre ;
- **[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.

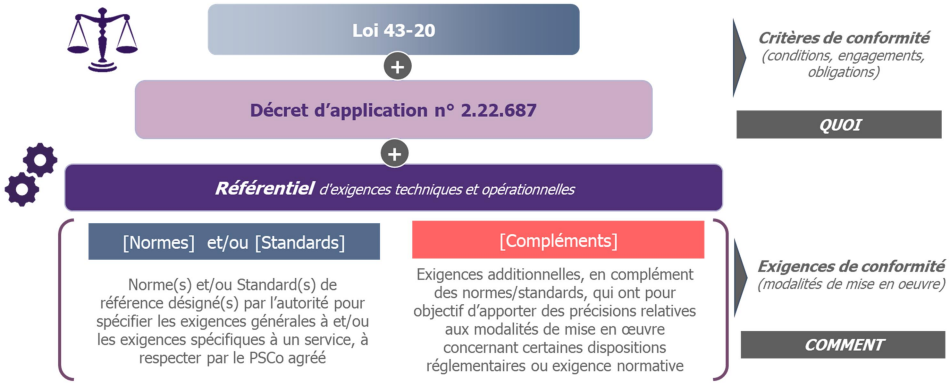

Figure 2 : Structure du cadre juridique et normatif.

4.2 Précautions 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 des normes reprises dans les référentiels, ont été élaborés 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** ;
- 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

Les principaux articles et dispositions de la loi n° 43-20 applicables spécifiquement aux PSCo agréés, indépendamment du service de confiance délivré, sont consolidés au niveau du tableau suivant :

	Article 32	Obligation de l'agrément du PSCo souhaitant fournir des services de confiance **qualifiés.**
	Article 33	Les conditions et les engagements à respecter pour devenir PSCo agréé + les obligations complémentaires en cas de délivrance de certificats qualifiés.

Chapitre Ier Section II *Des prestataires de services de confiance*	**Article 34**	Possibilité d'agréement des personnes morales de droit public pour fournir des services de confiance qualifiés.
	Article 36	Reconnaissance de PSCo qualifié étranger ou Service qualifié fournis depuis l'étranger dans le cadre d'un accord multilatéral ou bilatéral de reconnaissance réciproque entre le Maroc et le(les) pays hôte.
	Article 37	Les modalités/conditions d'arrêt de l'activité par un PSCo.
	Article 38	Obligation de non-divulgation des secrets professionnels pour le PSCo et ses employés.
	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.
	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.
Chapitre III *De l'autorité nationale …*	**Article 55**	Contrôle des activités des prestataires de service de confiance.
Titre III Dispositions … transitoires…	**Article 80**	Pour les PSCo précédemment agréés conformément aux dispositions de la Loi 53-05 : Délai maximum d'un an à compter de la date d'entrée en vigueur de la loi 43-20 pour se conformer aux dispositions de la nouvelle loi.

Tableau 1: *Récapitulatif des principaux articles et dispositions de la loi 43-20 relatifs aux PSCo agréés*

4.4 Rappel des principales dispositions du décret n°2.22.687 applicables

Les principaux articles et dispositions du décret n° 2.22.687 applicables spécifiquement aux PSCo agréés, indépendamment du service de confiance délivré, sont consolidés au niveau du tableau suivant :

Chapitre II **Section 1ère** Des prestataires de services de confiance agréés	**Article 13**	Modalités de soumission de la demande d'agrément, constituants du dossier (Annexe 2), et notification en cas de modification durant la période d'examen.
	Article 14	Demandeur d'agrément soumis, à ses frais, à une évaluation par un organisme désigné par l'autorité : contrôle du respect des conditions et des engagements L43-20 + les règles de sécurité applicables au service concerné. Rapport d'évaluation soumis au PSCo pour complétion.
	Article 15	Contenu de la décision d'agrément délivrée par l'autorité : Date ; Numéro ; Dénomination ; Service concerné ; Durée ; le cas échéants précision des Exigences restant à respecter.
	Article 16	Obligation d'informer l'autorité de toute modification de l'un des éléments au vu desquels l'agrément a été délivré.
	Article 17	Modalités de renouvellement de l'agrément (mêmes exigences que dossier initial + 4 mois avant la fin de validité).
	Article 18	Obligations de conservation des données relatives à la fourniture de service de confiance pour minimum 7 ans. Données à conserver ➔ renvoi vers les référentiels d'exigences.
	Article 19	Notification atteinte à la sécurité ou pertes d'intégrité : Obligation de respecter les modalités fixées dans le référentiel de gestion des incidents de cybersécurité publié par la DGSSI.
Chapitre V *Dispositions diverses*	***Article 32***	Publication des normes et référentiels applicables aux services de confiance, par l'autorité nationale sur son site Internet.

Tableau 2 : *Récapitulatif des principaux articles et dispositions du décret n° 2.22.687 relatifs aux PSCo agréés*

5 Procédure d'agrément

5.1 Modalités

L'agrément est exigé pour tout prestataire souhaitant fournir un service de confiance qualifié (article 32 - Loi 43-20).

L'agrément est forcément associé à la fourniture d'un service de confiance qualifié donné.

Les critères de conformité et les exigences associées conditionnant l'obtention de l'agrément sont précisés plus bas dans le document. Ils sont à compléter, de façon cumulative, par les exigences spécifiques relatives à chaque service qualifié que le prestataire souhaite délivrer.

Pour rappel, l'agrément est indépendant du certificat de conformité prévu au niveau des articles 8 et 17 de la loi n° 43-20. Ce dernier étant relatif aux dispositifs qualifiés de création de signature électronique ou de création de cachet électronique.

Cependant, tout dispositif, mis en œuvre par le PSCo demandeur de l'agrément, pour la création de signature électronique qualifiée ou la création de cachet électronique qualifié, doit disposer d'un certificat de conformité attestant sa qualification par l'autorité nationale. La liste des dispositifs qualifiés est publiée sur le site internet de l'autorité nationale (articles 8 et 17 – Loi n° 43-20).

Les modalités relatives à la procédure d'agrément sont précisées au niveau des articles 13, 14 et 15 du décret n° 2.22.687, à savoir :

- Dépôt physique du dossier de demande d'agrément auprès de l'autorité nationale ou envoi recommandé (postal ou électronique) :
  - Le formulaire de demande d'agrément, à compléter et soumettre, est publié par l'autorité nationale sur son site Internet, Les modalités de dépôt et d'envoi dudit dossier sont précisées au niveau de ce formulaire ;
  - Les documents constituant le dossier d'agrément sont précisés au niveau de l'annexe n° 2 du décret n° 2.22.687 ;
  - Un récépissé d'enregistrement de la demande est remis au PSCo candidat ;
- Communication à l'autorité nationale par le demandeur, de toute modification éventuelle survenue au cours de la phase d'examen du dossier de la demande d'agrément et affectant ce dernier :
  - Transmission des documents mis à jour en tenant compte des modifications survenues ;
- Evaluation sur pièce et sur place réalisée, aux frais du demandeur, par un organisme désigné et supervisé par l'autorité nationale :
  - Elaboration du rapport d'évaluation par l'organisme de contrôle puis transmission à l'autorité nationale et au demandeur pour compléter le dossier de sa demande ;
- Examen du dossier par l'autorité nationale suite au retour de l'organisme désigné :
  - Du fait de l'expertise technique nécessaire, et conformément à la loi 55-19 relative à la simplification des procédures et des formalités administratives et ses textes d'application, la durée de l'examen peut varier en fonction de l'étendue et de la complexité du système sous réserve de notification par l'autorité de confiance ;
  - A titre indicatif, la durée d'examen, dans le cas d'un dossier sans complexité spécifique, est estimée à 90 jours calendaires après le dépôt du dossier complet y compris le rapport d'évaluation par l'organisme de contrôle désigné ;

- Dans le cas de survenance d'une modification au cours de l'examen du dossier d'agrément, la durée d'examen est affectée en conséquence. L'autorité nationale réestime la durée nécessaire selon la nature des modifications survenues ;

- Délivrance de la décision d'agrément ; positive ou, le cas échéant, précision des exigences restant à respecter ;
- Si agrément accordé, publication par l'autorité nationale :
  - Au « Bulletin officiel », d'un extrait de la décision d'agrément (article 53, Loi 43-20) ;
  - Sur son site internet, dans la liste nationale des PSCo agréés par l'autorité nationale qui précise les PSCo agréés et les services qualifiés qu'ils délivrent (article 53, Loi 43-20).

Le rapport d'évaluation élaboré par l'organisme de contrôle doit permettre de démontrer le respect des exigences identifiées au niveau du présent référentiel [Ref_PSCo_AG] et notamment le respect de la norme EN 309 401.

Le formulaire d'intégration à la liste de confiance nationale, doit être annexé au rapport d'évaluation suivant les instructions précisées plus bas dans le présent document.

Une Certification ESTI EN 309 401 pourrait être jointe au rapport d'évaluation pour accélérer/simplifier l'examen.

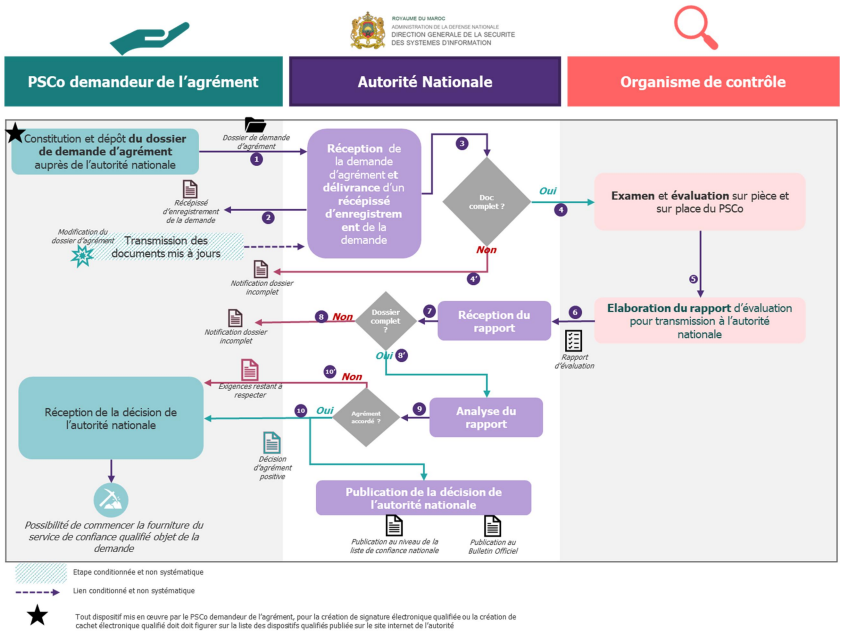

Figure 3 - Synthèse du processus d'agrément

Dans le cas où un PSCo agréé souhaite fournir un nouveau service qualifié autre que celui pour lequel il a été agréé initialement, et sauf demande explicite de l'autorité nationale, il est exempté de la fourniture des éléments administratifs **inchangés** qu'il a soumis lors de la précédente procédure d'agrément, à savoir :

- L'attestation d'inscription au registre du commerce, copie des statuts de la société et de son règlement intérieur ;
- La présentation générale du prestataire de service précisant : la répartition du capital, les activités et les types de services fournis, ses sites géographiques, son organisation et ses effectifs ;
- La liste des noms et qualités des dirigeants de la société ou des membres de son organe d'administration ainsi que la liste des personnes habilitées à agir en son nom ;

- La copie de la carte nationale d'identité de la personne chargée des formalités de la demande de l'agrément ou de tout document justifiant son identité ainsi que les documents attestant les pouvoirs qui lui sont conférés à cet effet ;
- La copie des cartes nationales d'identité électroniques du personnel du prestataire chargé de la gestion et de la fourniture du service de confiance ou de tout document justifiant leur identité et des diplômes ainsi que la description de leurs qualifications en la matière, accompagnée des documents justificatifs ;

5.2 Critères de conformité

En vue de l'obtention de l'agrément, 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, indépendamment du service qu'il souhaite délivrer, à savoir :

(Critère 1) Forme juridique conforme ; soit société de droit marocain (article 33.1.a de la Loi n°43-20) soit personne morale de droit public sous réserve de l'intérêt du service public (article 34 de la Loi n°43-20) ;

(Critère 2) Fiabilité et sécurité technique des systèmes, matériels et logiciels utilisés (article 33.1.b de la Loi n°43-20) ;

(Critère 3) Fiabilité de l'ensemble des processus mis en œuvre (article 33.1.b de la Loi n°43-20) ;

(Critère 4) Expérience et qualification du personnel et des sous-traitants le cas échéant, dans le domaine de la fourniture des services de confiance (article 33.1.c de la Loi n°43-20) ;

(Critère 5) Souscription à une assurance responsabilité civile couvrant les éventuels incidents et dommages résultant de sa faute professionnelle (article 33.1.d de la Loi n°43-20) ;

(Critère 6) Elaboration et maintien d'un plan de continuité d'activités intégral incluant un Plan de Reprise d'Activités (article 33.1.e de la Loi n°43-20) ;

(Critère 7) Précision exhaustive des conditions et limites d'utilisation des services de confiance avant l'établissement d'une relation contractuelle avec un futur client/utilisateur (article 33.2.a de la Loi n°43-20) ;

(Critère 8) Capacité de 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 (articles 33.2.b et 39 de la Loi n°43-20, article 18 du décret 2.22.687) ;

(Critère 9) Mise en place de procédures et de points de contrôles garantissant la notification de l'autorité nationale de toute modification de l'un des éléments au vu desquels l'agrément lui a été délivré (article 16 du décret 2.22.687) ;

(Critère 10) 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 (pour les PSCo délivrant des certificats électroniques ou des services basés sur les certificats) ;

(article 37 de la Loi n°43-20) ;

(Critère 11) Astreinte au secret professionnel pour le personnel et les sous-traitants du PSCo (article 38 de la Loi n°43-20) ;

(Critère 12) Mise en place des moyens et procédures, notamment de supervision et de gestion d'incidents, permettant de :

- Détecter au plus tôt toute atteinte à la sécurité ou toute perte d'intégrité ayant une incidence sur un service de confiance ou sur les données à caractère personnel qui y sont associés ;

› Notifier immédiatement après en avoir eu connaissance, l'autorité nationale et le cas échéant toute personne impactée par l'incident.

(Article 40 de la Loi n°43-20, article 19 du décret 2.22.687)

Les dispositions précisées au niveau des alinéas 2 et 3 de l'article 33 de la loi n° 43-20, concernant le service de délivrance de certificats électroniques qualifiés, ne sont pas abordés dans le présent document. Ils sont traités dans les référentiels d'exigences spécifiques.

A noter :

Le respect de ces critères* de conformité se matérialise par la mise en œuvre de la part du PSCo, des exigences de conformité listées plus bas dans le présent document (chapitre « Exigences de conformité »).

*en dehors du critère (1) administratif non couvert par la suite.

Certains critères (notamment les critères (2) et (3) relatifs à la fiabilité & sécurité technique des systèmes, matériels et logiciels utilisés et à la fiabilité des processus (article 33.1.b– Loi n°43-20) font également l'objet de précisions dans les référentiels d'exigences spécifiques applicables pour chaque service de confiance.

5.3 Validité et modification

La validité de l'agrément est de **trois (3) ans** au maximum (article 15 du décret n° 2.22.687).

Toute modification de l'un des éléments sur la base desquels l'agrément a été délivré doit être communiquée sans délai à l'autorité par le PSCo concerné (article 16 du décret n° 2.22.687).

Pour éviter toute suspension de l'agrément, il est fortement recommandé d'aviser l'autorité de nationale en amont de toute modification.

Les modifications envisagées ne doivent en aucun cas affecter la continuité du service de confiance qualifié fourni ou remettre en question les conditions et/ou engagements initiales d'attribution de l'agrément.

Si l'autorité nationale constate que les activités du PSCo agréé ne sont plus conformes aux dispositions de la loi 43-20 ou que les conditions initiales d'attribution de l'agrément ont été affectées, les dispositions de l'article 61 de la loi 43-20 s'appliquent ; à savoir :

- Mise en demeure avec un délai de remise en conformité (fixé par l'autorité) durant lequel l'agrément peut être suspendu par l'autorité ;
- Puis le cas échéant, retrait de l'agrément si non remise en conformité passé ce délai.

Dans le cas où la modification opérée est jugée comme étant majeure et pouvant affecter les conditions initiales d'attribution de l'agrément, l'autorité peut décider de suspendre l'agrément le temps de réexaminer le dossier.

NB : Des précisions relatives aux modifications concernées et aux modalités relatives à la notification de l'autorité, sont apportées plus bas dans le présent document (chapitre Exigences de conformité).

5.4 Renouvellement

Le renouvellement de l'agrément se fait selon les mêmes modalités prévues pour son obtention initiale.

Afin d'assurer la continuité de service et de maintenir le statut ininterrompu de l'agrément, il est fortement recommandé d'**anticiper au maximum la demande de renouvellement**.

Le délai de **quatre (4) mois** (avant la date d'expiration de l'agrément initiale) évoqué au niveau de l'article 17 du décret n° 2.22.687, est un délai minimum.

5.5 Disposition transitoire

La Loi 43-20 entre en vigueur à partir du 13/07/2023.

Un PSCE agréé au titre de la loi 53-05 dispose d'un délai de douze (12) mois pour se conformer aux dispositions de la Loi 43-20 et ses textes d'application :

- Cela inclut notamment la mise en conformité par rapport aux exigences du présent [Ref_PSCo_AG] ainsi que les autres référentiels adressant les services qualifiés que ledit PSCo fournit (article 80, Loi 43-20) ;
- Le délai de mise en conformité en question court à partir de la date d'entrée en vigueur de la Loi 43-20 (article 80, Loi 43-20).

Compte tenu de la date effective d'entrée en vigueur de la Loi 43-20 (13/07/2023), la date limite de mise en conformité pour les PSCE agréés au titre de la loi 53-05 est le **12/07/2024.**

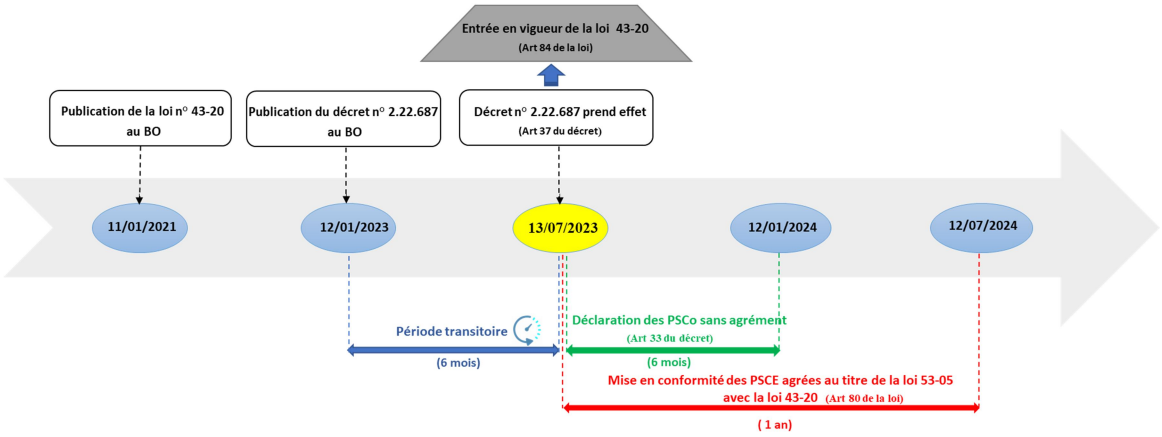

Figure 4 - Dates clés et délai de mise en conformité.

6 Exigences de conformité

Les exigences ci-après sont indépendantes du service de confiance fourni par le PSCo agréé.

Pour rappel, ces exigences, d'ordre général, sont complétées par des exigences spécifiques applicables à chaque service de confiance qualifié.

Ref_Psco_AG_Exig 1. Le PSCo agréé 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 une spécification dans l'une des normes et 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 procéder éventuellement à une rectification.

6.1 Norme ETSI EN 319 401

Ref_Psco_AG_Exig 2. Les PSCo agréés sont tenus de se conformer à l'ensemble des exigences de la norme ETSI EN 319 401 version v2.3.1 ou ultérieure. Cela comprend :

- Les exigences relatives à l'analyse des risques (*chap. 5 – Risk Assessment*) ;
- Les exigences relatives aux politiques & pratiques (*chap. 6 - Policies & parcticies*) y inclut :
  - Déclaration des pratiques du services de confiance (*6.1 Trust Service Practice statement) ;*
  - Conditions générales d'utilisation (6.2 *Terms and Conditions) ;*
  - Politique de sécurité de l'information (6.3 *Information security policy) ;*
- Les exigences relatives aux opérations et à la gestion du PSCo (*chap. 7 TSP Management and operations*) y inclut les modalités relatives aux sujets suivants :
  - Organisation interne *(7.1 Internal organization)* ;
  - Ressources humaines *(7.2 Human resources) ;*
  - Gestion des assets *(7.3 Asset management) ;*
  - Contrôle d'accès *(7.4 Access control) ;*
  - Contrôles cryptographiques *(7.5 Cryptographic controls) ;*
  - Sécurité physique et environnementale (*7.6 Physical and environmental security) ;*
  - Sécurité des opérations (*7.7 Operation security) ;*
  - Sécurité réseaux (*7.8 Network security) ;*
  - Gestion des incidents (*7.9 Incident management) ;*
  - Collecte des preuves (*7.10 Collection of evidence) ;*
  - Gestion de la continuité d'activités (*7.11 Business continuity management) ;*
  - Cessation/Arrêt d'activités du PSCo (*7.12 TSP termination and termination plans) ;*
  - Conformité vis-à-vis de la réglementation nationale (*7.13 Compliance) ;*

La norme ETSI 319 401 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.

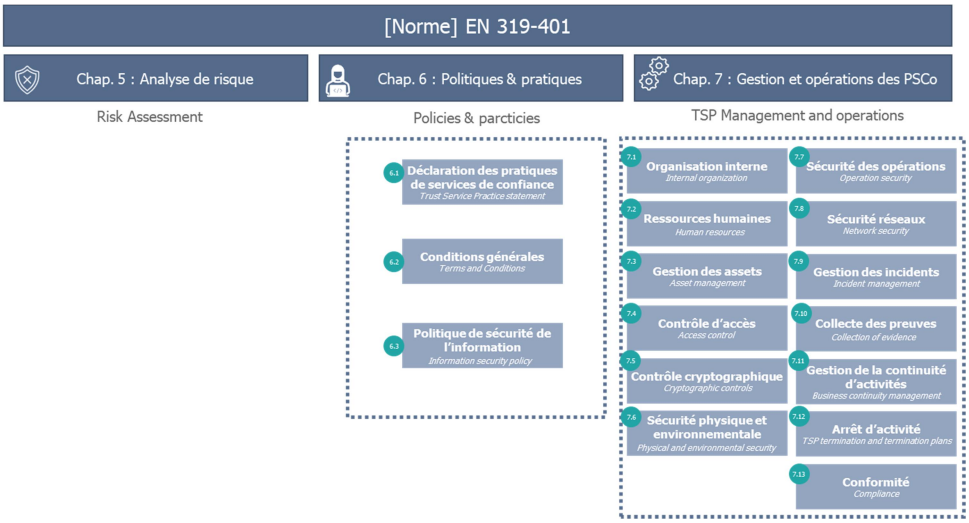

Figure 5 - Sujets couverts par la norme ETSI EN_319_401

6.2 Compléments à la norme ETSI EN 319 401

Les exigences de ce chapitre sont des compléments ou précisions en addition aux dispositions prévues au niveau des différents chapitres de la norme ETSI EN 319 401.

6.2.1 Analyse de risque (chapitre 5)

Ref_Psco_AG_Exig 3. L'analyse de risque doit couvrir tous les aspects du service de confiance à la fois techniques et non techniques. Elle doit être réalisée conformément à la norme ISO/CEI 27005 ou à une méthodologie équivalente validée au préalable par l'autorité nationale.

Ref_Psco_AG_Exig 4. Le rapport d'analyse de risque doit être joint au dossier de demande d'agrément.

Ref_Psco_AG_Exig 5. L'analyse de risque doit être formellement validée par la direction du PSCo agréé.

Ref_Psco_AG_Exig 6. Ladite analyse de risque et le rapport associé, doivent être mis à jour par le PSCo agréé :

- Systématiquement, au moins une fois par (1) an ;
- En cas d'évolution ou projet d'évolution ayant un impact significatif sur le service de confiance fourni par le PSCo agréé typiquement les évolutions qui sont susceptible d'affecter les la conformité du service qualifié fourni ;
- A la demande de l'autorité nationale, suite à la prise en compte des résultats de l'analyse d'impact soumise par le PSCo agréé à l'occasion d'une notification de modification ;

  Dans ces 2 derniers cas, l'analyse de risque doit être réalisée avant et après la réalisation de la modification :

  - **Avant** la réalisation pour prévoir l'impact et les actions de mitigations ;
  - **Après** la réalisation pour mesurer l'impact réel et mettre à jours les actions de mitigation.

6.2.2 Politique de Sécurité de l'Information (chapitre 6.3)

Ref_Psco_AG_Exig 7. La politique de sécurité de l'information doit être formellement approuvée par la direction avec une signature écrite ou électronique du représentant de la direction.

Ref_Psco_AG_Exig 8. Tous les employés concernés* doivent avoir accès à une documentation écrite ou électronique pour chaque procédure opérationnelle qu'ils peuvent être amenés à réaliser. Ils doivent également avoir accès aux politiques générales comme par exemple, les politiques de certifications applicables à une Autorité de Certification dans le cas de délivrance de certificats électroniques.

Les employés concernés sont ceux qui manipulent, administrent, développent ou opèrent un service de confiance ou un de ses composants. Il s'agit en particulier du personnel affecté à des rôles de confiance conformément à REQ-7.2-16 de la norme ETSI EN_319_401.

Ref_Psco_AG_Exig 9. La documentation doit être communiquée sur un support permanent. Cela peut être notamment : une documentation imprimée, l'accès à un référentiel web ou à un wiki, un document électronique fourni par courriel.

Ref_Psco_AG_Exig 10. Concernant la vérification des configurations des sous-systèmes de services de confiance au regard de la politique de sécurité, il est recommandé d'appliquer les recommandations du « CA/Browser Forum network Security Guide » :

- L'examen au moins une fois par semaine de la configuration de tous les sous-systèmes de services de confiance qualifiés.

Les sous-systèmes concernés dépendent du service de confiance délivré. Par exemple, pour un PSCo délivrant certificat, les configurations à examiner comprennent notamment : les systèmes de délivrance, les systèmes de gestion des certificats, les Systèmes de support de sécurité, les Systèmes de support…

6.2.3 Ressources humaines (chapitre 7.2)

Ref_Psco_AG_Exig 11. L'obligation de secret professionnel concerne, pour les PSCo, toute personne ayant des responsabilités relatives à un service de confiance (en particulier le personnel affecté à des rôles de confiance conformément à REQ-7.2-16 de la norme ETSI EN_319_401) et toute personne ayant une fonction de responsabilité managériale.

Ref_Psco_AG_Exig 12. L'obligation de secret professionnel du personnel doit se traduire formellement pour chaque employé ou intervenant concerné, par un engagement écrit et signé par la personne physique en question.

Ref_Psco_AG_Exig 13. Le PSCo agréé élabore et maintient un inventaire des rôles qui comprend notamment une liste de responsabilités clairement documentées. Pour chaque rôle, une correspondance claire doit être établie entre (le rôle) et ([la personne] ou [le groupe de personne]) responsable de ce rôle.

Ref_Psco_AG_Exig 14. Le PSCo agréé doit mettre en œuvre tous les moyens légaux dont il peut disposer pour s'assurer de l'honnêteté de son personnel affecté à des rôles de confiance (conformément à REQ-7.2-16 de la norme ETSI EN_319_401) ou à des fonctions de responsabilité. Le PSCo peut se baser notamment sur la fiche anthropométrique du futur employé pour vérifier l'absence de condamnation de justice potentiellement incompatible avec ses futures attributions dans un rôle de confiance. Cette vérification de compatibilité devrait ensuite être réalisée a minima une fois tous les trois (3) ans.

Ref_Psco_AG_Exig 15. Afin de garantir la non-répudiation, le PSCo agréé s'assure que toute personne ayant des responsabilités relatives à un service de confiance (en particulier le personnel affecté à des rôles de confiance conformément à REQ-7.2-16 de la norme ETSI EN_319_401) a préalablement accepté formellement les responsabilités qui lui sont confiées (par le biais d'un engagement écrit par exemple).

Ref_Psco_AG_Exig 16. Chaque employé et/ou sous-traitant doit signer un formulaire de confidentialité individuelle avant de pouvoir accéder à des informations confidentielles. Ce formulaire doit contenir a minima :

- Des informations relatives aux responsabilités légales et aux droits de l'employé ou du sous-traitant ;
- Les responsabilités liées à la classification des informations et à la gestion des actifs ;
- Les responsabilités des employés et/ou des sous-traitants ;
- Les actions de mitigations pouvant être réalisés par le PSCo agréé dans le cas de non-respect des mesures de confidentialité par les employés ou les sous-traitants.

Ref_Psco_AG_Exig 17. Les responsabilités en matière de sécurité de l'information doivent être clairement précisées avant d'établir toute relation contractuelle avec un futur employé ou un sous-traitant. Cela peut être réalisé notamment par :

- La précision des responsabilités en matière de sécurité dans l'offre d'emploi ou la description de poste ;
- La précision des exigences et des responsabilités en matière de sécurité dans les appels d'offres pour le choix de fournisseurs/sous-traitants.

Ref_Psco_AG_Exig 18. Le PSCo agréé doit faire en sorte que chaque employé suive, a minima une fois par an, une session de sensibilisation à la sécurité de l'information. Le contenu des actions de sensibilisation à la sécurité de l'information (formation, information) doit être conforme à sa politique de sécurité prédéfini. Par conséquent, le contenu doit être revu après chaque changement majeur de la politique de sécurité.

6.2.4 Asset Management (chapitre 7.3)

Ref_Psco_AG_Exig 19. L'inventaire des assets informatiques doit être mis à jour immédiatement après toute action modificative.

Ref_Psco_AG_Exig 20. Tous les assets informatiques ou catégories d'assets doivent être assignées à un responsable identifié.

Ref_Psco_AG_Exig 21. L'assignation des assets critiques tels que les HSM ou les cartes à puce administratives doit être acceptée par les employés par le biais d'un accord écrit ou équivalent (par exemple, un accord signé électroniquement).

Ref_Psco_AG_Exig 22. L'inventaire des assets critiques doit être vérifié tous les mois. L'inventaire des assets non critiques doit être vérifié sur une base annuelle.

6.2.5 Contrôles d'accès (chapitre 7.4)

Ref_Psco_AG_Exig 23. Une authentification forte est requise pour accéder aux ressources relatives à un service de confiance.

Ref_Psco_AG_Exig 24. Les membres du personnel affectés à des rôles de confiance conformément à REQ-7.2-15 de la norme ETSI EN_319_401, doivent disposer et utiliser des comptes utilisateurs nominatifs pour accéder à une ressource informatique (système, application, matériel, interface de supervision, interface de paramétrage …) relative à un service de confiance.

Ref_Psco_AG_Exig 25. Les journaux d'événements (logs) relatifs aux manipulations système par le personnel autorisé, doivent être conservés.

Ref_Psco_AG_Exig 26. L'accès aux journaux d'événements (logs) doit être sécurisé, tracé et strictement restreint. Les opérateurs systèmes (rôle de confiance conformément à la REQ-7.2-15 de la norme ETSI EN_319_401), ne doivent pas pouvoir accéder à ces journaux. La protection des journaux peut être réalisée par l'application d'un cachet électronique des journaux ou par des règles de restriction d'accès.

6.2.6 Contrôles cryptographiques (chapitre 7.5)

Ref_Psco_AG_Exig 27. Il est nécessaire de protéger les clés cryptographiques par une méthode impliquant au moins un double contrôle et une authentification à deux facteurs :

- Un contrôle basé par exemple sur un quorum de cartes à puce (typiquement 2 cartes parmi 5) est approprié pour couvrir à la fois le besoin de double contrôle et le besoin de disponibilité des opérateurs (n opérateurs parmi m doivent s'authentifier, avec n au moins égal à 2).

6.2.7 Sécurité réseau (chapitre 7.8)

Ref_Psco_AG_Exig 28. Les systèmes les plus critiques (tels que l'Autorité de Certification racine le cas échéant), ne doivent pas être exposés à l'extérieur. Ils doivent rester hors ligne (offline).

Ref_Psco_AG_Exig 29. De façon plus globale, l'exposition des services vers l'extérieur doit être limité et maîtrisé.

Ref_Psco_AG_Exig 30. Tous les systèmes doivent être protégés contre les attaques du réseau. Cela inclut des mesures telles que :

- Utilisation de pare-feu avec des configurations adéquates ;
- Délimitation des zones et séparation des composants dans des VLANs dédiés ;
- Application régulière et processée, de correctifs de sécurité sur les serveurs.

Ref_Psco_AG_Exig 31. L'utilisation de périphériques réseau certifiés est recommandée.

Ref_Psco_AG_Exig 32. L'authentification et la protection (intégrité/confidentialité) de la communication entre les composants est fortement recommandée avec des protocoles tels que TLS/SS.

Ref_Psco_AG_Exig 33. Il est recommandé que les serveurs de temps utilisés opèrent comme des serveurs NTP version 4 (NTP v4) conformément à la [RFC 5905].

6.2.8 Collecte des preuves (chapitre 7.10)

Ref_Psco_AG_Exig 34. Le PSCo agréé établit une convention de preuve qui définit les règles applicables au sein du service en matière de preuve notamment :

- La nature et portée des preuves produites ;
- Les modalités d'établissement des preuves ;
- Les modalités de conservation des preuves ;
- Les modalités de partage ou de mise à disposition des preuves, notamment en cas de désaccord
- Les modalités d'interprétation des preuves ;
- Les engagements contractuels des parties sur l'acceptation de la gestion des preuves électroniques.

Ref_Psco_AG_Exig 35. Il est recommandé de synchroniser tous les serveurs avec le même serveur NTP, de manière à éviter les potentielles dérives temporelles lors de la corrélation des journaux relatifs aux preuves.

Ref_Psco_AG_Exig 36. Les références de temps doivent respecter le format UTC (Coordinated Universal Time).

Ref_Psco_AG_Exig 37. Les serveurs Offline doivent être synchronisés avec un système d'horloge interne précis tel qu'une horloge temps réel (HTR) puisqu'ils ne peuvent pas être synchronisés avec un serveur NTP externe.

Ref_Psco_AG_Exig 38. Les dossiers de preuves doivent être scellés en appliquant un cachet électronique du prestataire à chaque dossier afin d'en renforcer la fiabilité et l'intégrité.

6.2.9 Continuité d'activité (chapitre 7.11)

Ref_Psco_AG_Exig 39. Le PSCo agréé doit mettre en place un Plan de Continuité d'Activités (incluant un Plan de Reprise d'Activités) en se référant à la norme ISO/IEC 27002 (version 2022 ou ultérieure).

Ref_Psco_AG_Exig 40. Le plan doit être maintenu, mis à jour régulièrement ou à l'occurrence de changement l'impactant.

Ref_Psco_AG_Exig 41. Le plan doit être intégralement testé par le PSCo agréé a minima une (1) fois par an.

Ref_Psco_AG_Exig 42. Un rapport sur l'exécution du plan doit être produit et les anomalies doivent être corrigées. Les corrections doivent êtres documentés.

6.2.10 Cessation d'activité (chapitre 7.12)

Ref_Psco_AG_Exig 43. Un plan de cessation d'activité doit être établi et mis à jour annuellement par le PSCo agréé. Son contenu doit respecter les exigences spécifiées au niveau du chapitre 7.12 de la norme ETSI EN 319_401 en question.

Ref_Psco_AG_Exig 44. En cas de cessation d'activité, 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 agréé maintient ou transfère, à un PSCo tiers fiable l'ensemble des moyens permettant d'assurer la continuité des fonctions critiques identifiées.

Il est fortement recommandé de pré-identifier le(s) prestataire(s) tiers potentiel(s) et de le(s) indiquer au niveau du plan de cessation d'activité.

6.2.11 Conformité (chapitre 7.13)

Il est entendu que le cadre légal de référence à considérer est bien 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).

Ref_Psco_AG_Exig 45. Le PSCo agréé est tenu de démontrer sa conformité par rapport à l'ensemble des dispositions de la loi n° 43-20 et ses textes d'application, notamment celles potentiellement non abordées explicitement dans les référentiels d'exigences publiés par l'autorité nationale.

6.3 Autres compléments et précisions

6.3.1 Conservation des données

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

En complément du chapitre « 7.10 Collecte de preuve » de la norme EN 319 401 et du complément associé spécifié plus haut.

Les données pertinentes à conserver concernant la fourniture d'un service de confiance dépendent de la nature du service fourni. Des précisions sont apportées dans les référentiels relatifs à chaque service.

Ref_Psco_AG_Exig 46. Le PSCo agréé doit utiliser des systèmes fiables pour conserver les données qui lui sont fournies, sous une forme vérifiable de manière que :

- L'authenticité de ces données puisse être vérifiée ;
- Seules des personnes autorisées puissent introduire et modifier les données conservées ;
- Les données ne soient publiquement disponibles pour des traitements qu'après avoir obtenu le consentement de la personne concernée par ces données.

Ref_Psco_AG_Exig 47. Les données pertinentes qui doivent être conservées sont toutes les informations relatives à la fourniture d'un service de confiance ou échangés avec le PSCo agréé dans le cadre de la réalisation d'une transaction électronique, et qui peuvent servir pour :

- Assurer la disponibilité et la continuité du service de confiance fourni y compris en cas d'arrêt de service ;
- Fournir des preuves suffisantes notamment en cas de litige ;
    - Des preuves de fiabilité du service confiance ;
    - Des preuves d'intégrité et de non-répudiation et de la transaction réalisée par le biais du service de confiance.

Cela comprend :

- Les conventions acceptées par l'utilisateur du service de confiance en particulier :
    - Les conventions de preuve ;
    - Les conditions d'utilisation du service ;
- Les éléments techniques du service de confiance qui ont servi à conclure la transaction électronique associée :
    - Le cas échéant, les certificats électroniques utilisés, l'ensemble des chaînes de certification mises en œuvre – certificats, jeton d'horodatage … ; les listes de révocation des certificats électroniques utilisées ;
- Les logs et pistes d'audit générées par les systèmes de fourniture du service de confiance notamment :
    - Les journaux d'événements (logs) relatifs aux manipulations système par le personnel autorisé ;
    - Le cas échéant, les éléments de traçabilité du workflow utilisé par le client pour utiliser le service de confiance ;
- Les politiques relatives aux services de confiance engagées (exemple : politique de certification, politique de signature …) :
    - Y compris les politiques relatives à des services fournis par des tiers intervenants dans la chaine de confiance (exemple : politique de certification dans le cas d'utilisation d'un certificat fourni par un PSCo tiers) ;
- Le descriptif des processus d'identification et d'enregistrement des clients ;
- Le cas échéant, les documents objet de la transaction après signature ou cachetage électroniquement, ou a minima les empreintes numériques (hash) de ces documents.

Ref_Psco_AG_Exig 48. Il est entendu que la conservation des données à caractère personnel doit se faire conformément aux 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). Le PSCo agréé s'engage 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 l'intéressé ;
- Ne traiter les données que dans le cadre des instructions et de l'autorisation reçues de l'intéressé ;
- 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 ou de toute société intervenant dans le cadre du traitement.

Ref_Psco_AG_Exig 49. Le PSCo agréé, met en œuvre les dispositions et moyens nécessaires afin de permettre à un client, justifiant de son identité et conformément à la législation en vigueur, de disposer du droit d'accès à ses données personnelles, du droit de rectification de celles-ci ainsi que du droit d'opposition, pour des motifs légitimes, au traitement de ses données.

Ref_Psco_AG_Exig 50. Le PSCo agréé doit démontrer les moyens mis en œuvre pour garantir la conservation et le maintien de l'accessibilité de ces données, pendant une période minimale de 7 ans y compris après un éventuel arrêt/cessation d'activité.

Ref_Psco_AG_Exig 51. Le PSCo agréé doit spécifier les procédures mises en place afin de garantir la suppression / destruction des données conservées à la fin de la période de conservation

6.3.2 Notification des modifications

[Précisions relatives aux dispositions des articles 16 du décret 2.22.687]

Ref_Psco_AG_Exig 52. Le PSCo agréé met en place des procédures et points de contrôles garantissant la notification de l'autorité nationale de toute modification concernant l'un des éléments au vu desquels l'agrément lui a été délivré (article 16 du décret 2.22.687).

Ces modifications comprennent notamment, sans s'y limiter :

- Changement au niveau de la prise de participation du prestataire de service de confiance ;
- Modification d'une des informations publiées au niveau de la LNPA (Liste Nationale des PSCo Agréés) ;
- Changements de procédures d'enregistrement ;
- Changements de procédures d'identification ;
- Changements induits par une modification de la politique de service ;
- Changements induits par une modification des conditions générales d'utilisation d'un service ;
- Changements de sous-traitants ;
- Modifications des conditions d'hébergement des services ;
- Changements de composant technique matériel ou logiciel relatif à la fourniture du service de confiance ;
- Changements de matériels cryptographiques ;
- Modifications d'architecture technique ;
- Changements dans la gouvernance du prestataire de service ;
- Modifications entrainant des changements dans la liste de confiance publiée par l'autorité nationale.

La notification ne concerne pas les changements dits standards au sens ITILv4 (Information Technology Infrastructure Library version 4) à savoir : les modifications de système prédéfinis et préapprouvés à faible risque et à faible impacts.

Ne sont pas concernées non plus les applications de patchs et mises à jour logiciels correctifs et les évolutions de workflows ou de paramétrages n'impactant pas le chemin de preuve et les composants associés (autorité de certification, modules cryptographiques…).

Ref_Psco_AG_Exig 53. Le PSCo agréé doit définir et maintenir à jour une liste de changements SI techniques ou paramétriques standards au sens ITILv4 (Information Technology Infrastructure Library version 4) à savoir les changements prédéfinis à faible risque et à faible impacts, qui ne sont pas de nature à remettre en question les conditions initiales d'attribution de l'agrément.

Ref_Psco_AG_Exig 54. La notification de modification doit être accompagnée :

- D'un rapport d'analyse des impacts relatifs à la mise en œuvre de la modification concernée ;
- D'une analyse de risque mise à jour dans le cas d'une évolution significative.

Ref_Psco_AG_Exig 55. La notification de modification se fait soit par envoi recommandé (postale ou électronique) ou par dépôt contre récépissé auprès de l'autorité nationale. Le PSCo agréé transmet également des versions mises à jour de tous les documents impactés par les modifications réalisées.

- Les documents transmis par **voie postale** sont à adresser à :

Administration de la Défense Nationale
Direction Générale de la Sécurité des Systèmes d'Information (DGSSI)
Direction de la Stratégie et de la Réglementation (DSR)
Méchouar, 10090, Rabat.

Ces documents peuvent être transmis par **voie électronique** au courrier électronique suivant:

PSCo-dsr@dgssi.gov.ma

Dans ce cas, les documents contenant des données sensibles et/ou confidentielles peuvent être transmis par voie électronique en chiffrant les documents avec un moyen convenu avec l'autorité nationale.

6.3.3 Assurances

[Précisions relatives aux dispositions de l'article 33.1.d – Loi n°43-20]

Ref_Psco_AG_Exig 56. Le prestataire et ses sous-traitants, souscrivent et maintiennent en vigueur pendant toute la durée d'exercice de leurs activités de fourniture de service de confiance, une assurance couvrant a minima les risques de responsabilité civile, d'accident de travail et de multirisques d'exploitation ou tout autre :

- Responsabilité civile exploitation ;
- Responsabilité civile produits après livraison ;
- Responsabilité civile professionnelle.

Ref_Psco_AG_Exig 57. Il est recommandé que le montant de l'assurance soit au minimum égal à 3 fois la valeur du chiffre d'affaires annuel prévu par le prestataire relativement à ses activités de PSCo. Le PSCo agréé doit faire parvenir régulièrement à l'autorité nationale une copie de ces polices d'assurance (renouvellements ou nouvelles souscriptions) avant leurs dates d'échéance contractuelle (dates de fin de la couverture).

Ref_Psco_AG_Exig 58. Le PSCo agréé supporte seul les conséquences d'un manquement de ses sous-traitants à satisfaire aux obligations d'assurances (souscription et montant).

6.3.4 Modules cryptographiques utilisés

Ref_Psco_AG_Exig 59. Les modules cryptographiques utilisés pour les fonctions fixées dans les différents référentiels spécifiques aux services qualifiés, doivent se conformer aux exigences suivantes :

- **Certification et évaluation** : les modules cryptographiques concernés doivent être certifiés conformément aux spécifications suivantes :
  - **Obligatoire - Common Criteria version 3 ou ultérieure :**
    - 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) ;
  - **Fortement recommandé - FIPS 140-3 ou ultérieure : niveau de certification 3 ou supérieur :**
    - Les produits certifiés selon la norme FIPS 140-2 restent valables jusqu'à la date d'expiration fixée par le FIPS (généralement 5 ans après leur date de validation et au plus tard le 21 septembre 2026) ;
- **Protection des clés et des données** : les modules cryptographiques concernés doivent garantir la protection des clés et des données sensibles. Ils doivent offrir des mécanismes de génération de clés sécurisés, de stockage sécurisé des clés et de protection contre les attaques physiques et logiques ;
- **Algorithmes et protocoles sécurisés** : les modules cryptographiques concernés doivent prendre en charge des algorithmes et des protocoles cryptographiques sécurisés et reconnus ;
- **Mises à jour et gestion des vulnérabilités** : les modules cryptographiques concernés doivent être maintenus à jour pour remédier aux vulnérabilités connues et aux failles de sécurité. Les correctifs et des mises à jour régulières doivent être appliqués pour assurer la sécurité continue des modules.

6.3.5 Algorithmes et mécanismes cryptographiques

Ref_Psco_AG_Exig 60. Les algorithmes et mécanismes cryptographiques mis en œuvre doivent être conformes aux spécifications définies au niveau de la norme ETSI TS 119 312 (v1.4.2 ou ultérieure) Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.

6.3.6 Formats autorisés des signatures/cachets électroniques et conteneurs associés

Pour toutes les signatures/cachet avancées ou qualifiées utilisés par les PSCo agréé dans le cadre de la fourniture des services de confiance qualifiés.

Ref_Psco_AG_Exig 61. Les formats autorisés, pour les signatures électroniques avancées et/ou qualifiées et pour les cachets électroniques avancés et/ou qualifiés, ainsi que pour les conteneurs associés, 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 associés :

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

6.3.7 Publication sur la liste nationale des PSCo agréés

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

L'autorité nationale s'appuiera sur les recommandations du standard ETSI TS 119_612 pour l'élaboration et la publication de la **LNPA (Liste Nationale des PSCo Agréés)**. Elle précisera les PSCo agréés et les services qualifiés qu'ils fournissent.

La liste sera publiée au format PDF mais également au format XML pour les services qualifiés.

La liste de confiance XML des services qualifiés sera cachetée (ou signée) électroniquement par l'autorité nationale (ou un agent de l'autorité nationale) afin d'en garantir l'intégrité et la source.

L'utilisation, par les PSCo agréé et par l'autorité, des canevas standards prévus par la [TS_119_612] permet de répondre à plusieurs enjeux notamment :

- Permettre d'évaluer le niveau de confiance qui peut être accordé à un service de confiance donné ;
- Permettre la mise en place des services de validation de signature/et ou cachet électronique ;
- Faciliter la collaboration entre les prestataires de services de confiance ;
- Permettre la reconnaissance mutuelle avec des PSCo établis en dehors du territoire national.

Ref_Psco_AG_Exig 62. L'identification du PSCo doit respecter les exigences définies dans la clause 5.4 du standard [TS_119_612].

Ref_Psco_AG_Exig 63. L'identification d'un service de confiance dans la liste LNPA doit respecter les exigences définies dans la clause 5.5 du standard [TS_119_612].

Ref_Psco_AG_Exig 64. En particulier, le PSCo demandeur de l'agrément complétera le formulaire « [Ref_PSCo_AG] Formulaire_publication_Liste LNPA » relatif à l'intégration dans la liste de confiance LNPA qui lui sera transmis par l'autorité au cours de la demande d'agrément.

7 Annexes

Liens vers les normes et standards

- **ETSI EN 319 401**: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers:
  - **Se référer à la version la plus récente** publiée sur le site de l'ETSI :

    https://www.etsi.org/deliver/etsi_en/319400_319499/319401/
  - 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_319499/319401/02.03.01_60/en_319401v020301p.pdf

- **ETSI TS 119 612** Electronic Signatures and Infrastructures (ESI); Trusted Lists :
  - **Se référer à la version la plus récente** publiée sur le site de l'ETSI :

    https://www.etsi.org/deliver/etsi_ts/119600_119699/119612/
  - 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_ts/119600_119699/119612/02.02.01_60/

- **ETSI TS 119 312** Electronic Signatures and Infrastructures (ESI); Cryptographic Suites :
  - **Se référer à la version la plus récente** publiée sur le site de l'ETSI :

    https://www.etsi.org/deliver/etsi_ts/119300_119399/119312/
  - A titre indicatif, la version la plus récente au moment de la rédaction du présent document est la suivante (v1.4.2) :

    https://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.04.02_60/ts_119312v010402p.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/