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

Référentiel relatif aux services de confiance non qualifiés et aux prestataires fournissant ces services

[Ref_Serv_Conf_NonQual]

Normes et compléments applicables aux services de confiance non qualifiés et aux prestataires qui les fournissent

Suivi des mises à jour du document [Ref_Serv_Conf_NonQual]

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

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

PSCo-dsr@dgssi.gov.ma

Sommaire

1 Terminologie et acronymes

AC : Autorité de certification.

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

Autorité Nationale 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).

Certificat LCP : *Lightweight Certificate Policy ;* certificat conforme à la politique de certificat de niveau LCP conformément à la norme ETSI 319 411-1 imposant notamment une vérification de l'identité du titulaire du certificat par rapport à une pièce d'identité et des CGU signés par le titulaire du certificat.

Certificat NCP : *Normalized Certificate Policy ;* certificat conforme à la politique de certificat de niveau NCP conformément à la norme ETSI 319 411-1 imposant notamment les exigences du certificat LCP complétées par une preuve d'un face à face avec le titulaire du certificat.

Certificat NCP+ : *Extended Normalized Certificate Policy* ; certificat conforme à la politique de certificat de niveau NCP+ conformément à la norme ETSI 319 411-1 imposant notamment les exigences du certificat NCP complétées par l'obligation de l'utilisation d'un dispositif cryptographique sécurisé.

CGU : Conditions Générales d'Utilisation.

ERDS *(Electronic Registered Delivery Service)* Service d'envoi recommandé électronique.

http : hypertext transfer protocol.

ITILv4 ou ultérieure : Information Technology Infrastructure Library version 4 (ou ultérieure).

Liste Déclarative des PSCo fournissant des services Autres que Qualifiés (LDPAQ) : désigne, conformément à l'article 53 de la Loi 43-20, la liste déclarative des prestataires de services de confiance délivrant des services autres que qualifiés et ayant réalisé la déclaration de fourniture de services de confiance auprès de l'autorité conformément à l'article 35 de la Loi 43-20.

OID : *Object Identifier.*

PC : Politique de Certification.

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

PSCo sans agrément : désigne un PSCo non agréé au sens de la loi 43-20, qui fournit un (ou plusieurs) service(s) de confiance autre(s) que qualifié(s) conformément à la Loi n° 43-20.

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

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

REMS *(Registered Electronic Mail Service)* Service d'envoi de courrier électronique recommandé ; est un service d'envoi recommandé électronique structuré autour de formats, protocoles et mécanismes utilisés dans les services de messagerie électronique.

UTC : Temps Universel Coordonné (Coordinated Universal Time).

Utilisateur : désigne l'utilisateur final (personne moral ou physique) du service de confiance (titulaire du certificat électronique, signataire, créateur d'un cachet électronique …).

2 Objet et périmètre

Le présent document **[Ref_Serv_Conf_NonQual]** constitue le référentiel fixant les normes, standards et compléments applicables aux services de confiance **non qualifiés** et aux PSCo qui les fournissent, conformément au cadre légal national rappelé dans le présent document notamment au niveau du chapitre « Cadre de référence » .

Le respect des exigences du présent référentiel [Ref_Serv_Conf_NonQual] conditionne la conformité des services de confiance non qualifiés ci-après ainsi que la conformité des PSCo qui les fournissent :

- La création des certificats électroniques relatifs aux signatures électroniques avancées et/ou aux cachets électroniques avancés ;
- La création du service d'horodatage électronique simple ;
- La création du service d'envoie recommandé électronique simple ;

Pour les PSCo fournissant les autres services de confiance non qualifiés (en dehors de ceux précisés ci-dessus), **le respect des exigences du présent référentiel [Ref_Serv_Conf_NonQual] est fortement recommandé** (en particulier les chapitres 6.1.1 et 6.2).

Conformément aux articles 52, 54 et 55, le contrôle de la conformité des activités des PSCo non agréés est assurée par l'autorité nationale.

3 Modalités de mise à jour

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

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

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

4 Cadre de référence

4.1 Cadre juridique et normatif

Le cadre légal de référence auxquels sont soumis les prestataires de services de confiance délivrant des services de confiance autres que qualifiés 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, le présent document explicite, quand cela est nécessaire, les modalités organisationnelles et techniques pour la mise en œuvre des dispositions précitées, en s'appuyant sur des :

- **[Normes]** et/ou **[Standards]** de référence désignés par l'autorité pour spécifier :
  - Les exigences générales à respecter par le PSCo indépendamment du service de confiance non qualifié qu'il fournit ;
  - Les exigences spécifiques à un service de confiance non qualifié donné.
- **[Compléments]** Ensemble d'exigences ou de spécifications additionnelles, en complément des normes/standards 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 Précautions d'interprétation des normes et standards ETSI

Les normes et standards ETSI (et potentiellement 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 utilisées, 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 ;
- Les termes "**EU Advanced Electronic Signature**" ou "**Advanced** electronic **Signature**" sont à transposer en **signature électronique avancée** au sens de la loi 43-20 **;**
- Les termes "**EU Advanced Electronic Seal**" ou "**Advanced** electronic **Seal**" sont à transposer en **cachet électronique avancé** au sens de la loi 43-20 **;**
- Le terme **« EU qualified »** est à transposer en **:**
  - **« Agréé »** lorsqu'il s'agit d'un **PSCo** (hors périmètre du présent document) ;
  - **« Qualifié »** lorsqu'il s'agit d'un **service de confiance ou d'un certificat électronique** (Nota Bene : un certificat qualifié peut être utilisé pour fournir un service de confiance non qualifié) ;
- 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

En sus des dispositions générales applicables à l'ensemble des PSCo, le tableau ci-après consolide les principaux articles et dispositions de la loi n° 43-20 applicables spécifiquement aux services de confiance autres que qualifiés et/ou aux PSCo qui les fournissent :

Titre préliminaire **Dispositions générales**	**Article 2**	Définition, au sens de la Loi 43-20, notamment des éléments suivants : - Signature électronique simple ; - Données de création de signature électronique ; - Certificat de signature électronique ; - Dispositif de création de signature électronique ; - Cachet électronique simple ; - Données de création de cachet électronique ; - Certificat de cachet électronique ; - Dispositif de création de cachet électronique ; - Prestataire de services de confiance.
Chapitre Ier Section I[ère] ***Des services de confiance*** Sous-section première. ***De la signature électronique***	**Article 4**	Introduction de 3 niveaux pour la signature électronique : Une signature électronique est une signature soit simple, soit avancée ou qualifiée.
	Article 5	Définition d'une signature électronique avancée Une signature électronique avancée est une signature électronique simple qui satisfait aux conditions suivantes : (1) être propre au signataire ; (2) permettre d'identifier le signataire ; (3) avoir été créée à l'aide de données de création de signature électronique que le signataire peut utiliser sous son contrôle exclusif, avec un niveau de confiance élevé défini par l'autorité nationale ; (4) reposer sur un certificat électronique ou tout procédé jugé équivalent fixé par voie réglementaire ; (5) et être liée aux données associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable.
	Article 7	Effet juridique et recevabilité d'une signature électronique simple ou avancée comme preuve en justice.
Chapitre Ier Section I[ère] ***Des services de confiance*** Sous-section 2 ***Du cachet électronique***	**Article 13**	Introduction de 3 niveaux pour le cachet électronique : Un cachet électronique est un cachet soit simple, avancé ou qualifié.
	Article 14	Définition du cachet électronique avancé : Un cachet électronique avancé est un cachet électronique simple qui satisfait aux conditions suivantes : (1) être propre au créateur du cachet de manière univoque ; (2) permettre d'identifier le créateur du cachet ; (3) avoir été créé à l'aide de données de création de cachet électronique que le créateur du cachet peut utiliser sous son contrôle, avec un niveau de confiance élevé défini par l'autorité nationale ; (4) reposer sur un certificat électronique ou tout procédé jugé équivalent fixé par voie réglementaire ; (5) et être lié aux données auxquelles il est associé de telle sorte que toute modification ultérieure des données soit détectable.
	Article 16	Effet juridique et recevabilité d'un cachet électronique simple ou avancé comme preuve en justice.
Chapitre Ier	**Article 22**	Introduction de 2 niveaux d'horodatage électronique : Un horodatage électronique est un horodatage simple ou qualifié.

Section I[ère] ***Des services de confiance*** Sous-section 3 ***De l'horodatage électronique***	**Article 23**	Définition de l'horodatage simple : L'horodatage électronique simple consiste en des données sous forme électronique qui associent d'autres données sous forme électronique à un instant particulier et établissent la preuve que ces dernières données existaient audit instant.
	Article 25	Effet juridique et recevabilité d'un horodatage électronique simple comme preuve en justice.
Chapitre Ier Section I[ère] ***Des services de confiance*** Sous-section 4 ***Du service d'envoi recommandé électronique***	**Article 26**	Introduction de 2 niveaux pour un service d'envoie recommandé électronique : Un service d'envoi recommandé électronique est un service d'envoi recommandé électronique simple ou qualifié.
	Article 27	Définition du service d'envoie recommandé électronique simple : Le service d'envoi recommandé électronique simple permet de transmettre des données par voie électronique, fournit des preuves concernant le traitement des données transmises, y compris la preuve de leur envoi et de leur réception, et protège les données transmises contre les risques de perte, de vol, d'altération ou de toute modification non autorisée.
	Article 29	Effet juridique et recevabilité des données envoyées et reçues à l'aide d'un service d'envoi recommandé électronique simple comme preuve en justice.
Chapitre Ier Section II ***Des prestataires de services de confiance***	**Article 35**	Obligation de déclaration préalable auprès des autorités pour toute personne qui se propose de fournir des services de confiance autres que qualifiés.
	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 Et les cas pour lesquels l'obligation du secret professionnel ne peut être invoquée.
	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 Ier Section III **Des obligations du titulaire de certificat électronique**	**Article 42**	Obligation pour le titulaire du certificat de notifier, au plus tôt, le PSCo de toute modification des informations contenues dans ce certificat électronique.
	Article 43	Obligation pour le titulaire du certificat de faire révoquer ce dernier immédiatement en cas de doute sur : - la perte de la confidentialité relative aux données afférentes à la création de la signature/cachet électronique ; - ou la perte de conformité à la réalité pour les informations contenues dans le certificat.
	Article 44	Obligation pour le titulaire d'un certificat électronique de ne plus l'utiliser dès lors que ce dernier (le certificat) arrive à échéance ou qu'il a été révoqué.
Chapitre III **De l'autorité nationale …**	**Article 52**	Les normes et référentiels applicables aux services de confiance sont fixés par l'autorité nationale.
	Article 53	Publication par l'autorité sur son site internet de la liste des PSCo non agréés ayant effectué leurs déclarations préalables prévues à l'article 35 de la Loi 43-20.
	Article 55	Soumission des PSCo au contrôle de l'autorité afin de vérifier la conformité de leurs activités quant aux dispositions de la Loi 43-20 et des textes pris pour son applications. Les frais inhérents aux opérations de contrôle sont à la charge du PSCo.

Tableau 1: *Récapitulatif des principaux articles et dispositions de la loi 43-20 relatifs aux services de confiance autres que qualifiés et aux PSCo qui les fournissent.*

4.4 Rappel des principales dispositions du décret n° 2.22.687 applicables

En sus des dispositions générales applicables à l'ensemble des PSCo, le tableau ci-après consolide les principaux articles et dispositions du décret n° 2.22.687 applicables spécifiquement aux services de confiance autres que qualifiés et/ou aux PSCo qui les fournissent :

Chapitre III *Des prestataires de services de confiance*	**Article 18** (Et article 23)	Obligations de conservation des données relatives à la fourniture de service de confiance pour minimum 7 ans. Données à conserver ➔ renvoi vers le présent référentiel d'exigences.
	Article 19 (Et article 23)	Notification en cas d'atteinte à la sécurité ou de pertes d'intégrité : obligation de respecter les modalités fixées dans le référentiel de gestion des incidents de cybersécurité publié par la DGSSI.
	Article 21	Modalités relatives à la déclaration préalable des prestataires fournissant des services autres que qualifiés ; constituants du dossier (annexe 3) ; et notification en cas de modification des éléments déclarés.
	Article 22	Modalités de validation de procédés jugés équivalents au certificat électronique pour les services (signature et cachet électroniques) avancés en application des articles 5 et 14 de la Loi 43-20 : - étude technique par l'autorité démontrant l'équivalence entre le procédé proposé et le certificat électronique en termes de sécurité et de fiabilité ; - précision dans un arrêté des procédés jugés équivalent.
	Article 23	Applicabilité des articles 18 et 19 aux PSCo fournissant des services de confiance autres que qualifiés.
Chapitre IV *Dispositions diverses*	***Article 32***	Publication des normes et référentiels applicables aux services de confiance, par l'autorité nationale sur son site Internet.
	Article 33	Pour les PSCo fournissant des services autres que qualifiés : Délai maximum de douze (12) mois après la publication du décret au bulletin officiel pour se conformer à ses dispositions.

Tableau 2 : *Récapitulatif des principaux articles et dispositions du* ***décret n° 2.22.687,*** *relatifs aux services de confiance autres que qualifiés et aux PSCo qui les fournissent.*

5 Procédure de déclaration

5.1 Modalités

Une déclaration préalable est exigée pour tout prestataire souhaitant fournir un service de confiance autre que qualifié *(article 35 - Loi 43-20).*

La déclaration est forcément associée à la fourniture d'un service de confiance donné.

Les critères et les exigences conditionnant la conformité du prestataire souhaitant fournir un service autre que qualifié, sont précisés dans le présent document.

Les modalités relatives à la déclaration préalable sont précisées au niveau de l'article 21 du décret n° 2.22.687, à savoir :

- Dépôt physique de la déclaration préalable auprès de l'autorité nationale ou envoi recommandé (postal ou électronique) :
  - Le formulaire de déclaration préalable, à compléter et soumettre, est publié par l'autorité nationale sur son site Internet. Les modalités de dépôt et d'envoi du dossier sont précisées au niveau de ce formulaire ;
  - Les documents constituant la déclaration sont précisés au niveau de l'annexe n° 3 du décret n° 2.22.687 ;
  - Un récépissé de réception de la demande est remis au PSCo déclarant.
- Communication à l'autorité nationale par le déclarant, de toute modification éventuelle affectant un des éléments de la déclaration :

Il est recommandé de compléter le dossier de déclaration préalable (précisé au niveau de l'annexe n° 3 du décret n°2.22.687) par des éléments attestant du respect des exigences du présent [Ref_Serv_Conf_NonQual] et en particulier le respect des normes qui y sont référencés pour les services fournis par le PSCo (par exemple : une certification ETSI EN319 401 serait un plus).

Le PSCo déclarant n'est pas tenu d'attendre un retour de la part de l'autorité nationale pour fournir les services de confiances non qualifiés qui ont fait l'objet de sa procédure déclarative.

Cependant l'autorité nationale peut à tout moment, conformément aux dispositions de la Loi 43-20 (notamment les articles 52, 54, 55 et 56) :

- Demander des précisions, des éléments explicatifs ou des documents complémentaires permettant à l'autorité de mieux apprécier la conformité des activités du PSCo ;
- Inviter le PSCo à des ateliers / séances d'écoute ;
- Procéder à un contrôle a posteriori afin de vérifier la conformité des activités du PSCo et des services de confiance qu'il fournit par rapport aux différentes dispositions de la Loi 43-20, des textes pris pour son application et des exigences de conformité décrites dans le présent document :
  - Ce contrôle peut se faire sur place et/ou sur pièce selon la nature des services fournis ;
  - Ce contrôle n'est pas systématique et sera déclenché par l'autorité nationale sur la base d'éléments qu'elle jugera pertinents ;
  - L'autorité peut avoir recours à des experts, au frais du déclarant, pour la réalisation de sa mission de contrôle.

⇨ Un rapport est établi à l'issue de la mission de contrôle. Les conclusions sont partagées avec le PSCo pour rectification/ajustement/correction.

⇨ **Selon la nature des éventuels écarts de conformité constatés, l'autorité peut spécifier, sur la liste publiée sur son site** (la liste déclarative des PSCo fournissant des services autres que Qualifiés) **le caractère non conforme du PSCo concerné, jusqu'à remédiation.**

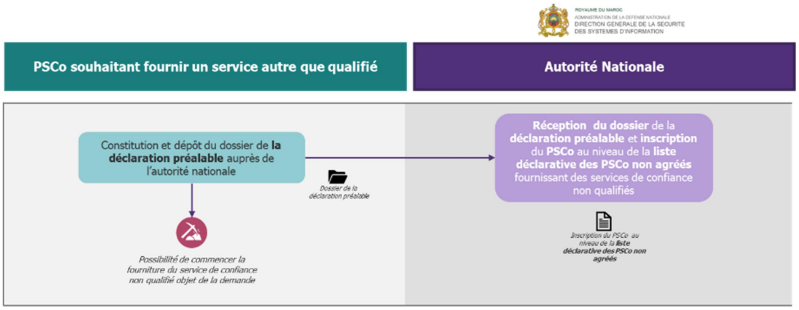

Figure 2 - Procédure de déclaration préalable

Dans le cas où, un PSCo non agréé déjà déclaré, souhaite fournir un nouveau service autre que celui concerné par sa déclaration préalable, 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 :

- La copie des statuts de la société ;
- L'attestation d'inscription au registre de commerce ;
- 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 copie de la carte nationale d'identité électronique de la personne chargée des formalités de la déclaration ou de tout document justifiant son identité, ainsi que les documents justifiant les pouvoirs qui lui sont conférés à cet effet.

5.2 Modification

Toute modification de l'un des éléments au vu desquels la déclaration a été réalisée doit être communiquée à l'autorité nationale, dans les meilleurs délais, par le PSCo déclarant (article 21 du décret n° 2.22.687).

Il est fortement recommandé d'aviser l'autorité de nationale en amont de toute modification.

Les modifications envisagées ne doivent pas affecter la fiabilité et la sécurité du service de confiance fourni.

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).

5.3 Disposition transitoire

Un PSCo non agréé qui délivre un service de confiance autre que sécurisé au sens 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 (article 33 du décret n° 2.22.687) :

- **Le délai de mise en conformité en question court à partir de la date de publication du décret n° 2.22.687 au bulletin officiel ;**
- Cela inclut notamment la **mise en conformité par rapport aux exigences du présent document**.

Compte tenu de la date de publication du décret n° 2.22.687 au Bulletin Officiel (12/01/2023), la date limite de mise en conformité pour les PSCo non agréés au titre de la loi 53-05 est le **12/01/2024.**

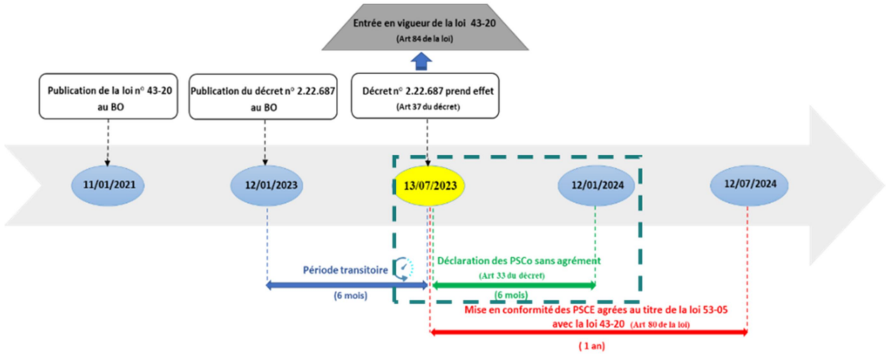

Figure 3 - Dates clés et délai de mise en conformité

6 Exigences de conformité

La déclaration préalable et les contrôles a posteriori, doivent démontrer la conformité du PSCo par rapport aux exigences de conformité listées au niveau du présent chapitre.

Ref_Serv_Conf_NonQual_Exig 1. Le PSCo 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 Normes applicables

Le tableau suivant présente la **liste des normes applicables** aux services de confiance non qualifiés et aux prestataires qui les fournissent :

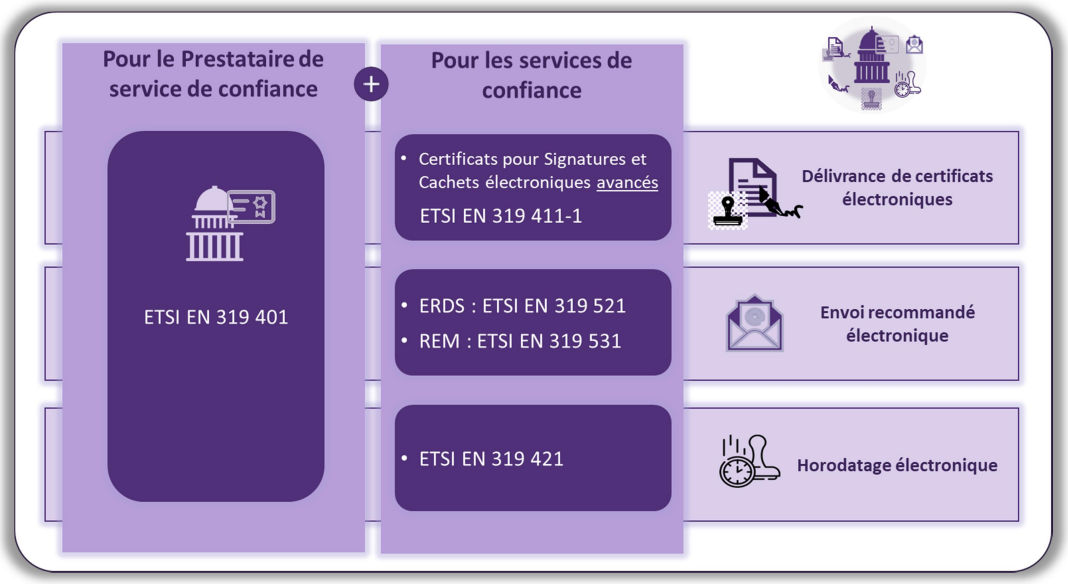

Figure 4 - Normes applicables aux services de confiance non qualifiés et aux prestataires qui les fournissent

Nota Bene :

Au niveau des normes, certaines exigences et/ou chapitres spécifiques, faisant mention de prestataires ou services « EU Qualified », s'adressent explicitement aux PSCo agréées.

Sauf indication contraire notamment au niveau des compléments, ces exigences ne sont pas imposées aux services non qualifiés et aux PSCo qui les fournissent.

6.1.1 Norme applicable à tous les PSCo

Ref_Serv_Conf_NonQual_Exig 2. Les PSCo sont tenus de se conformer aux exigences de la norme ETSI EN 319 401 (version v2.3.1 ou ultérieure) indépendamment du service autre que qualifié qu'ils fournissent. Cela inclut :

- Les exigences relatives à l'analyse des risques (*chap. 5 – Risk Assessment*)
- Les exigences relatives aux politiques & pratiques (*chap. 6 - Policies & parcticies*) y inclut
  - Les modalités relatives aux déclarations des pratiques de services de confiance (*6.1 Trust Service Practice statement)*
  - Les modalités relatives à l'élaboration des conditions générales d'utilisation (6.2 *Terms and Conditions)*
  - Les modalités relatives à la 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 présent document.

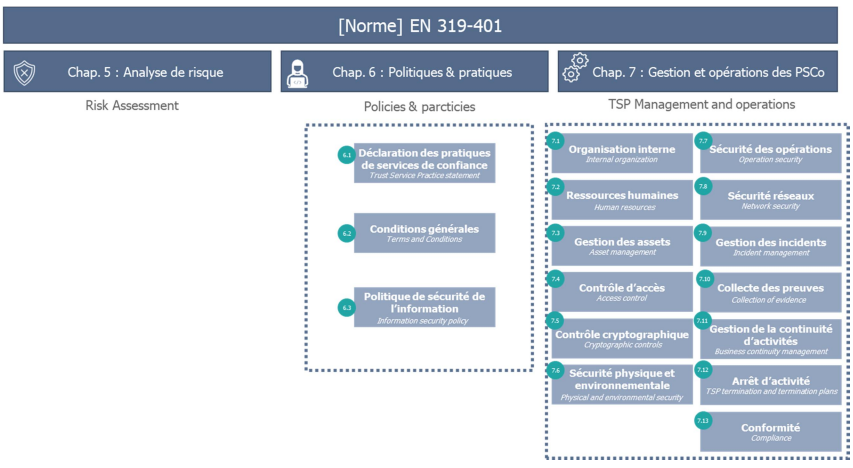

Figure 5 – Synthèse des sujets couverts par la norme ETSI EN 319 401

6.1.2 Normes spécifiques par service de confiance

Certificats électroniques pour service de confiance avancé

Ref_Serv_Conf_NonQual_Exig 3. Le PSCo souhaitant fournir des certificats électroniques pour signature électronique avancée et/ou cachet électroniques avancé, est tenu de respecter les exigences de la norme ETSI EN 319 411-1 (v1.3.1 ou ultérieure) :

- *ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI) ; Policy and security requirements for **Trust Service Providers issuing certificates**; Part 1: **General requirements.***

Horodatage électronique simple

Ref_Serv_Conf_NonQual_Exig 4. Le PSCo, souhaitant fournir un **service d'horodatage électronique,** est tenu de se conformer aux exigences de la norme **ETSI EN 319 421** (v1.2.1 ou version ultérieure) :

- *ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers **issuing Time-Stamps.***

Envoi recommandé électronique simple

Ref_Serv_Conf_NonQual_Exig 5. Le PSCo, souhaitant fournir un service **d'envoie recommandé électronique**, est tenu de respecter :

- Spécifiquement, les exigences de la norme **ETSI EN 319 531** (v1.2.1 ou ultérieure) dans le cas de la fourniture d'un **service REMS** (Electronic Registered Delivery Service) :
  - *ETSI EN 319 531 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for **Registered Electronic Mail Service** Providers.*
- Plus généralement, les exigences de la norme **ETSI EN 319 521** (v1.1.1 ou ultérieure) dans le cas de la fourniture d'un **service ERDS** (Registered Electronic Mail Service) **autre que REMS :**
  - *ETSI EN 319 521 Electronic Signatures and Infrastructures (ESI);Policy and security requirements for **Electronic Registered Delivery Service** Providers.*

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

6.2.1 Cas de la Signature/cachet électronique avancé

[Compléments aux dispositions des articles 5 et 14 de la Loi 43-20]

Ref_Serv_Conf_NonQual_Exig 6. Le certificat électronique sur lequel repose la signature électronique avancé (article 5 de la Loi 43-20) ou le cachet électronique avancé (article 14 de la Loi 43-20) doit être **conforme à la norme ETSI EN 319 411-1 ou à la norme ETSI EN 319 411-2** :

- Autrement dit, une signature électronique avancée (ou un cachet électronique avancé) doit reposer a minima **sur un certificat ETSI LCP** au sens de la norme **ETSI EN 319 411-1 ;**
- Une signature électronique avancée (ou un cachet électronique avancé) peut également reposer sur un certificat **ETSI NCP** ou **NCP+** ou **QCP** au sens des normes **ETSI EN 319 411-1/2.**

Ref_Serv_Conf_NonQual_Exig 7. Pour les **signatures électroniques avancées** le procédé utilisé pour la création de signature doit garantir que les clés de signature sont utilisées sous le contrôle exclusif du signataire avec un niveau de confiance élevé.

- Pour assurer le respect de cette exigence, l'utilisation des clés de signature par le signataire autorisé doit être réalisée au travers **d'une authentification forte multi-facteurs** du signataire mettant en œuvre **au moins 2 facteurs d'authentification.**

Ref_Serv_Conf_NonQual_Exig 8. Pour les **cachets électroniques avancées** le procédé utilisé pour la création du cachet doit garantir que les clés de cachet sont utilisées sous le contrôle du créateur du cachet avec un niveau de confiance élevé :

- Pour assurer le respect de cette exigence, l'utilisation des clés de cachet par le créateur autorisé du cachet doit être réalisée au travers d'une authentification forte du créateur du cachet.

Ref_Serv_Conf_NonQual_Exig 9. La signature électronique avancée (ou cachet électronique avancé) doit être liée (lié) aux données associées à cette signature (ce cachet) de telle sorte que toute modification ultérieure des données soit détectable :

- Le respect de cette exigence peut être réalisée par l'application d'une **fonction de hachage** conforme aux exigences du chapitre **« Algorithmes et mécanismes cryptographiques ».**

Ref_Serv_Conf_NonQual_Exig 10. La vérification de l'identité d'un utilisateur, au vu de la création du certificat électronique de signature électronique avancée ou de cachet électronique avancé, peut être déléguée par le PSCo à une autorité d'enregistrement tierce ou à un partenaire tiers (sous-traitant) en charge uniquement de la vérification de l'identité. Dans ce cas :

- Un contrat doit obligatoirement être établi préalablement pour :
  - Lier le PSCo au tiers ;
  - Encadrer les relations, préciser les obligations, rôles et responsabilités du tiers ;
  - Préciser les moyens de contrôle mis en place pour permettre au PSCo de vérifier la conformité et le respect des engagements du tiers ;
  - Les modalités d'établissement des preuves de vérification de l'identité.
- La politique de certification doit spécifier clairement le rôle du tiers et le procédé utilisé pour la vérification de l'identité ;
- Le PSCo doit être en capacité de :
  - Contrôler, à tout moment, les procédés utilisés par le tiers (et plus globalement contrôler le respect de sens engagements contractuels dans le cadre de la fourniture du service de confiance) ;
  - Apporter les preuves/garanties du respect des exigences du présent référentiel (notamment le respect des exigences de la norme ETSI EN 319 411-1).

Ref_Serv_Conf_NonQual_Exig 11. Il va sans dire que, les dispositions de vérification de l'identité au vu de la délivrance d'un certificat qualifié, telles que précisées au niveau du référentiel [Ref_Deliv_Cert_Qual] restent applicables (suffisants mais pas nécessaires) pour la délivrance de certificats non qualifiés conformes ETSI EN 319 411-1 (en particulier les certificats de type NCP et NCP+).

Procédé alternatif au certificat électronique

Ref_Serv_Conf_NonQual_Exig 12. Conformément à l'article 22 du décret n° 2.22.687, la mise en œuvre d'un procédé alternatif (équivalent) au certificat électronique dans le cadre de la fourniture de services de confiance (signature ou cachet électroniques) avancés, **est soumis à un accord préalable de l'autorité nationale** et à une publication de ce(s) procédé(s) dans **un arrêté :**

- Le PSCo souhaitant mettre en œuvre un procédé alternatif doit au préalable soumettre à l'autorité un dossier technique détaillé décrivant le procédé proposé et démontrant l'équivalence avec le certificat électronique en termes de fiabilité et de sécurité.
- Ce dossier doit contenir une analyse de risque couvrant les éventuelles menaces relatives à l'utilisation de ce procédé alternatif en remplacement du certificat électronique ;
- Une démonstration (proof of concept) pourrait être exigée par l'autorité ;
- Le dossier peut être renforcé par :
    - Le renvoi à des normes/standards internationaux reconnus ;
    - La mise en avant de cas d'adoptions similaires dans des contextes internationaux ayant un niveau d'exigences, en termes de services de confiance, comparable au contexte national.

L'autorité analyse les éléments soumis, demande éventuellement des compléments de précision avant de statuer sur l'équivalence ou non du procédé proposé.

6.2.2 Dossier de preuves

[Complément au chapitre Collecte des preuves (chapitre 7.10) de la norme ETSI 319 401]

Ref_Serv_Conf_NonQual_Exig 13. Le PSCo 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_Serv_Conf_NonQual_Exig 14. Il est fortement recommandé de sceller les dossiers de preuves en appliquant un cachet électronique du prestataire à chaque dossier afin d'en renforcer la fiabilité et l'intégrité.

6.2.3 Conservation des données

[Précisions relatives aux dispositions des articles 18 et 23 du décret 2.22.687].

En complément du chapitre « 7.10 Collecte de preuve » de la norme E319 401 et des éléments précisés pour chaque service de confiance concerné au niveau des normes ETSI EN 319 411-1 / EN 319 421 / EN 319 531 et EN 319 521.

Les éléments précisés dans ce chapitre sont cumulatifs avec les éléments précisés par service au niveau de la norme associée concernant les données pertinentes à conserver pour ledit service.

Ref_Serv_Conf_NonQual_Exig 15. Le PSCo doit utiliser des systèmes fiables pour conserver les données qui lui sont fournies, sous une forme vérifiable de manière à ce 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_Serv_Conf_NonQual_Exig 16. 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 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/cessation de service ;
- Fournir des preuves suffisantes notamment en cas de litige notamment :
    - 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 ;
- Le descriptif des processus d'identification/authentification et d'enregistrement de l'utilisateur du service de confiance :
    - Y compris, le cas échéant, les conventions établies entre le PSCo et des tiers intervenant dans l'enregistrement des utilisateurs ou la vérification de leur identité (exemples : autorité d'enregistrement déléguée, sous-traitant en charge de l'enrôlement et de la vérification de l'identité des utilisateurs au vu de l'émission du certificat de signature ou de cachet...) ;
- Les Dossiers d'enregistrement y compris les dossiers de preuve vérification de l'identité des utilisateurs, leurs justificatifs d'identité et, le cas échéant, de leurs entités de rattachement… ;
- 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 intervenant dans la chaine de confiance (exemple : politique de certification dans le cas d'utilisation d'un certificat fourni par un PSCo tiers) ;
- 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 suivi par l'utilisateur dans le cadre de l'utilisation du service de confiance ;
- 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_Serv_Conf_NonQual_Exig 17. 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). Afin de garantir le secret, la sécurité et la confidentialité des données, le PSCo (et/ou ses partenaires tiers) s'engage en particulier à :

- Préserver la sécurité et l'intégrité des données, notamment empêcher qu'elles ne soient déformées, endommagées et empêcher d'empêcher toute utilisation détournée, malveillante ou frauduleuse des données traitées ;
- Empêcher tout accès ou publication qui ne soit pas préalablement autorisé par l'utilisateur du service de confiance ;
- Ne traiter les données que dans le cadre des instructions et de l'autorisation reçues de l'utilisateur ;
- 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 prestataire ou de toute société intervenant dans le cadre du traitement.

Ref_Serv_Conf_NonQual_Exig 18. Le PSCo, met en œuvre les dispositions et moyens nécessaires afin de permettre à un utilisateur, 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_Serv_Conf_NonQual_Exig 19. Le PSCo doit garantir la conservation et le maintien de l'accessibilité de ces données, **pendant une période de 7 ans y compris après un éventuel arrêt (cessation) d'activité**.

Ref_Serv_Conf_NonQual_Exig 20. Le PSCo doit garantir la suppression / destruction des données conservées à la fin de la période de conservation.

6.2.4 Notification des modifications

[Précisions relatives aux dispositions aux article 16 et 21 du décret 2.22.687]

Ref_Serv_Conf_NonQual_Exig 21. Le PSCo met en place des procédures et points de contrôles garantissant la notification de l'autorité nationale, dans les meilleurs délais, des modifications concernant l'un des éléments au vu desquels la déclaration préalable a été réalisée (article 21 du décret 2.22.687)

Ces modifications comprennent notamment :

- Changement au niveau de la prise de participation du PSCo ou au niveau de sa gouvernance ;
- Changement (significatif) des procédures d'enregistrement ou procédures d'identification des utilisateurs ;
- Modification d'une des informations déclaratives publiées sur la LDPAQ (Liste Déclarative des PSCo fournissant des services Autres que Qualifiés) ;
- Changement induit par une modification de la politique de service ;
- Changement induit par une modification des conditions générales d'utilisation d'un service ;
- Changement de sous-traitants ;
- Changement de composant technique matériel ou logiciel relatif à la fourniture du service de confiance notamment les composants cryptographiques ;
- Modification des conditions d'hébergement des services ;
- Modifications d'architecture technique.

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, HSM…).

Ref_Serv_Conf_NonQual_Exig 22. Le PSCo doit définir et maintenir à jour une liste de changement 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.

Ref_Serv_Conf_NonQual_Exig 23. La notification de modification doit être accompagnée d'un rapport d'analyse des impacts relatifs à la mise en œuvre de la modification concernée.

Ref_Serv_Conf_NonQual_Exig 24. 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 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.

Indiquer : Notification de modification – PSCo non agréé.

Ces documents peuvent être transmis par voie électronique au courrier électronique ci-dessous :

PSCo-dsr@@dgssi.gov.ma

Objet : Notification de modification – PSCo non agréé.

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.

6.2.5 Formats autorisés des signatures/cachets électroniques et conteneurs associés

Ref_Serv_Conf_NonQual_Exig 25. Les formats autorisés, pour les signatures électroniques avancées et pour les cachets électroniques avancés, 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.

6.2.6 Algorithmes et mécanismes cryptographiques

Ref_Serv_Conf_NonQual_Exig 26. 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.

6.2.7 Publication sur la liste déclarative des PSCo fournissant des services autres que qualifiés

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

Conformément à l'article 53 de la Loi 43-20, l'autorité nationale publie sur son site internet, **une Liste Déclarative des PSCo** fournissant des services de confiance **Autres** que **Qualifiés (LDPAQ).**

Nota Bene :

- **L'autorité se base sur les informations déclarées par le PSCo ;**
- **Le PSCo est pleinement responsable de l'exactitude des informations déclaratives transmises à l'autorité** et qui sont retranscrites par l'autorité sur son site internet au niveau de ladite liste LDPAQ ;
- **L'autorité ne procède pas systématiquement à un contrôle préalable de l'ensemble des informations déclarées par le PSCo** ;
- **La publication sur le site de l'autorité ne vaut en aucun cas une preuve de la conformité du PSCo déclaré ;**
- **Cependant, en cas de réalisation d'une mission de contrôle mettant en lumière une absence de conformité du PSCo et selon la nature des écarts de conformité constatés, l'autorité peut, indiquer sur ladite liste, le caractère non conforme du PSCo concerné, jusqu'à remédiation.**

Ref_Serv_Conf_NonQual_Exig 27. Le PSCo s'engage à garantir l'exactitude et le maintien à jour des informations déclaratives transmises à l'autorité et qui sont retranscrites sur son site internet au niveau de la liste LDPAQ.

Ref_Serv_Conf_NonQual_Exig 28. Le PSCo précisera avec soin, au niveau du formulaire de déclaration préalable publié par l'autorité nationale sur son site Internet, les informations suivantes qui seront publiées sur ladite liste déclarative LDPAQ :

- Dénomination officielle ou raison sociale du prestataire telle qu'enregistrée auprès des autorités compétentes ;
- Numéro d'immatriculation officiel du PSCo (ICE, numéro d'inscription au registre du commerce, …) ;
- Adresse postale du PSCo ;
- Adresse électronique du PSCo ;
- URL du PSCo ;
- Pour chaque service de confiance fourni :
  - Type de service de confiance ;
  - Nom « commercial » du service ;
  - Bref descriptif du service ;
  - OID du service ;
  - URI vers la politique du service (exemple : politique de certification, politique d'horodatage…).

7 Annexes

Liens vers les normes et standard

- **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 EN_319 411-1 :** Electronic Signatures and Infrastructures (ESI) ; Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
  - **Se référer à la version la plus récente** publiée sur le site de l'ETSI **:**

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

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

- **ETSI EN 319 421 :** Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.
  - Se référer à la version la plus récente publiée sur le site de l'ETSI **:**
    https://www.etsi.org/deliver/etsi_en/319400_319499/319421/
  - A titre indicatif, la version la plus récente au moment de la rédaction du présent document est la suivante (v1.2.1) :

    https://www.etsi.org/deliver/etsi_en/319400_319499/319421/01.02.01_60/en_319421v010201p.pdf

- **ETSI EN 319 521 :** Electronic Signatures and Infrastructures (ESI); Policy and security requirements for **Electronic Registered Delivery Service** Providers.
  - **Se référer à la version la plus récente** publiée sur le site de l'ETSI :

    https://www.etsi.org/deliver/etsi_en/319500_319599/319521/
  - A titre indicatif, la version la plus récente au moment de la rédaction du présent document est la suivante (v1.1.1) :

    https://www.etsi.org/deliver/etsi_en/319500_319599/319521/01.01.01_60/en_319521v01 0101p.pdf

- **ETSI EN 319 531 :** Electronic Signatures and Infrastructures (ESI); Policy and security requirements for **Registered Electronic Mail Service** Providers.

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

  https://www.etsi.org/deliver/etsi_en/319500_319599/319531

- A titre indicatif, la version la plus récente au moment de la rédaction du présent document est la suivante (v1.1.1) :

  https://www.etsi.org/deliver/etsi_en/319500_319599/319531/01.01.01_60/en_319531v01 0101p.pdf