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

4

[Ref_Env_reco_Qual]

Exigences de conformité des prestataires fournissant un service **d'envoi recommandé électronique qualifié**

Suivi des mises à jour du document [Ref_Env_Reco_Qual]

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

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

PSCo-dsr@dgssi.gov.ma

Sommaire

1 Terminologie et acronymes

AC : Autorité de certification

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

ERDS (Electronic Registered Delivery Service) **:** Service d'envoi recommandé électronique permettant de transmettre des données entre un émetteur et un destinataire par voie électronique, offrant des preuves de transmission des données notamment au travers de preuves d'envoi et de réception et garantissant une protection des données transmises des risques perte, vol ou modification

QERDS (Qualified ERDS) **:** Service d'envoi recommandé électronique qualifié au titre de la loi 43-20

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

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

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

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

QREMS (Qualified REMS) **:** Service d'envoi de courrier électronique recommandé qualifié au titre de la loi 43-20 (QREMS est un service QERDS particulier)

2 Objet et périmètre

Le présent document, désigné par **[Ref_Env_Reco_ Qual]**, constitue le référentiel fixant les exigences de conformité à respecter par les PSCo agréés fournissant un **service d'envoi recommandé électronique qualifié** et ce conformément au **cadre légal national** rappelé dans le présent document notamment au niveau du chapitre « Cadre de référence ».

Le respect des exigences des référentiels [Ref_Env_Reco_Qual] & [Ref_PSCo_Ag] conditionnent l'obtention de l'agréement pour la fourniture du service d'envoi recommandé électronique qualifié.

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

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

3 Modalités de mise à jour

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

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

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

4 Cadre normatif

4.1 Cadre juridique et normatif

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

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

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

- Pour le service **QERDS (Qualified Electronic Registered Delivery Service):**

  [Norme] EN 319 521 v1.1.1 (2019-02) ou version ultérieure **:** Electronic Signatures and Infrastructures ESI); Policy and security requirements for Electronic Registered Delivery Service Providers.

- Plus spécifiquement, pour le service **QREMS** (**Qualified Registered Electronic Mail Service) :**

  [Norme] EN 319 531 v1.1.1 (2020-07) ou version ultérieure **:** Electronic Signatures and Infrastructures (ESI) ; Policy and security requirements for Registered Electronic Mail Service Providers.

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

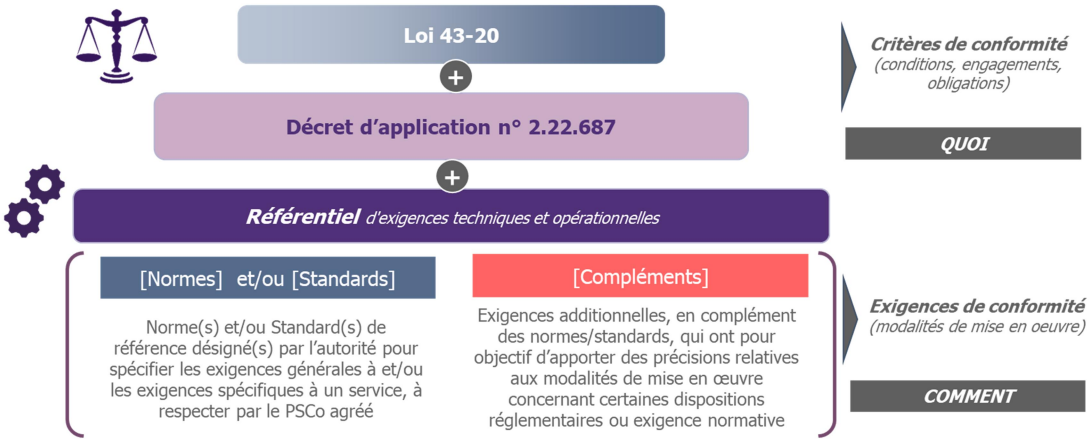

Figure 1 : Structure du cadre juridique et normatif

4.2 Précaution d'interprétation des normes et standards ETSI

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

L'utilisation de ce cadre présente un double avantage :

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

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

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

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

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

En sus des dispositions générales applicables à l'ensemble des PSCo, les principaux articles et dispositions de la loi n° 43-20 applicables spécifiquement aux PSCo agréés fournissant un **service d'envoi recommandé qualifié**, sont consolidés au niveau du tableau suivant :

Chapitre Ier **Section Ière** *Des services de confiance* **Sous-section 4** *Du service d'envoi recommandé électronique*	**Article 27**	Définition du service d'envoi recommandé électronique simple *(socle pour la définition du service d'envoi recommandé qualifié) :* - 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 28	Définition du service d'envoi recommandé électronique qualifié : Le service d'envoi recommandé électronique qualifié est un service d'envoi recommandé électronique simple qui satisfait aux conditions suivantes : (1) être fourni par un ou plusieurs PSCo agréé(s) ; (2) garantir l'identification de l'expéditeur avec un degré de confiance élevé, défini par l'autorité nationale ; (3) garantir l'identification du destinataire avant la fourniture des données ; (4) sécuriser l'envoi et la réception de données par une signature électronique avancée ou par un cachet électronique avancé, de manière à exclure toute possibilité de modification indétectable des données ; (5) signaler clairement à l'expéditeur et au destinataire toute modification des données nécessaire pour l'envoi ou la réception de celles-ci ; (6) indiquer par un horodatage électronique qualifié, la date et l'heure d'envoi et de réception ainsi que toute modification des données.
Chapitre Ier **Section II** *Des prestataires de service de confiance*	**Article 32**	Obligation d'agréement : seuls les PSCo agréés peuvent fournir un service* de confiance qualifié et gérer les opérations y afférentes. * ici le service d'envoi recommandé électronique qualifié.
	Article 33	Utilisation, dans le cadre de la fourniture du service* de confiance qualifié, de systèmes, matériels et logiciels fiables ; et garantie de leur sécurité technique et de la fiabilité des processus pris en charge. * ici le service d'envoi recommandé électronique qualifié.
	Article 39	Obligation pour le PSCo de conserver les données relatives à la fourniture du service* de confiance. Le cas échéant obligation de les communiquer aux autorités judiciaires en informant la partie utilisatrice. * ici le service d'envoi recommandé électronique qualifié.
	Article 40	Obligation de notification en cas d'atteinte à la sécurité ou perte d'intégrité relative à un service* ou à des données à caractères personnelles. * ici le service d'envoi recommandé électronique qualifié.

Tableau 1: *Récapitulatif des principaux articles et dispositions de la loi 43-20 relatifs au service d'envoi recommandé électronique qualifié*

4.4 Rappel des principales dispositions du décret n° 2.22.687 applicables

En sus des dispositions générales applicables à l'ensemble des PSCo, les principaux articles et dispositions du décret n° 2.22.687 applicables spécifiquement aux PSCo agréés fournissant des services d'**envoi recommandé électronique qualifié**, sont consolidés au niveau du tableau suivant :

Chapitre Ier **Section Ière** Des services de confiance qualifiés	**Article 5**	Obligation pour le PSCo fournissant un service d'envoi recommandé électronique qualifié, de procéder à la vérification de l'identité de l'expéditeur et du destinataire conformément aux dispositions du présent référentiel.
	Article 6	Preuve de dépôt par l'expéditeur : Obligation pour le PSCo de : - délivrer à l'expéditeur une preuve du dépôt électronique dès réception (par le PSCo) des données objet de l'envoi recommandé ; - conserver ladite preuve de dépôt pendant au moins un an. Cette preuve de dépôt comporte les informations suivantes : – pour l'expéditeur : prénom et nom ou dénomination, adresse électronique ; – pour le destinataire : prénom et nom ou dénomination, adresse électronique ; – un numéro d'identification unique de l'envoi attribué par le PSCo ; – la date et l'heure du dépôt des données objet de l'envoi indiquées par un horodatage électronique qualifié ; – la signature électronique avancée ou le cachet électronique avancé, utilisé par le PSCo lors de l'envoi.
	Article 7	Preuve de réception par le destinataire : La preuve de réception par le destinataire des données envoyées comporte : - les informations contenues dans la preuve de dépôt (article 6) ; - la date et l'heure de l'envoi et de la réception, indiquées par un horodatage électronique qualifié. Obligation pour le PSCo de conserver la preuve de réception pendant au moins 1 an. Preuve de refus ou de non-réclamation par le destinataire : Obligation pour le PSCo de remettre à l'expéditeur, après l'expiration d'un délai convenu avec ce dernier, la preuve de refus de réception ou de non-réclamation par le destinataire le cas échéant. La preuve de refus doit préciser : - les informations contenues dans la preuve de dépôt (article 6) ; - la date et l'heure du refus indiquées par un horodatage électronique qualifié. Obligation pour le PSCo de conserver la preuve de refus ou de non-réclamation du destinataire pendant au moins 1 ans à compter de la date de son établissement. Accès aux informations L'expéditeur a accès aux informations mentionnées au présent article pendant un an.
Chapitre II **Section Ière** Des prestataires de services de confiance agréés	**Article 13**	Constituants du dossier d'agrément (Annexe 2) relatifs au service* confiance qualifié ; Obligation de notification en cas de modification durant la période d'examen. * ici le service d'envoi recommandé électronique qualifié.
	Article 18	Obligation pour le PSCo de conserver des données relatives à la fourniture des services* de confiance qualifiés sur une période de 7 ans. Renvoi vers les référentiels d'exigences pour spécifier les types des données à conserver. * ici le service d'envoi recommandé électronique qualifié.

Tableau 2 : *Récapitulatif des principaux articles et dispositions du décret n° 2.22.687 relatifs au service d'envoi recommandé électronique qualifié*

5 Procédure d'agrément

Pour un PSCo souhaitant fournir un service d'envoi recommandé électronique qualifié.

5.1 Modalités

Le processus d'agrément d'un PSCo pour la fourniture d'un service d'envoi recommandé électronique qualifié est décrit au niveau du référentiel **[Ref_PSCo_AG].**

Les critères de conformité et les exigences associées, conditionnant l'obtention de l'agrément pour la fourniture d'un service d'envoi recommandé électronique qualifié, sont précisés plus bas dans le présent document. Ils sont à compléter, de façon cumulative, par les exigences de conformité du référentiel **[Ref_PSCo_AG].**

5.2 Critères de conformité

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

(Critère 1) Être agréé : seul un (ou plusieurs) PSCo agréé(s) au titre de la loi 43-20 et ses textes d'applications, peut (peuvent) fournir un service d'envoi recommandé qualifié et gérer les opérations y afférentes (article 32 et article 28 de la loi 43-20) ;

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

(Critère 3) Protéger les données transmises contre les risques de perte, de vol, d'altération ou de toute modification non autorisée (article 27 de la loi 43-20) ;

(Critère 4) Assurer la fiabilité des processus mis en œuvre (article 33 de la loi 43-20) ;

(Critère 5) Préciser de façon exhaustive les conditions et limites d'utilisation du service de confiance qualifié (ici service d'envoi recommandé qualifié) avant l'établissement d'une relation contractuelle avec un futur client/utilisateur (article 33.2.a de la loi 43-20) ;

(Critère 6) Garantir la conservation pendant sept (7) ans, de manière sécurisée avec accès contrôlé et limité (publication soumise à consentement de l'intéressé), des données pertinentes concernant les échanges relatifs au service d'envoi recommandé électronique qualifié.

Garantir la conservation pendant 1 an minimum, de la preuve de dépôt, la preuve de réception et le cas échéant la preuve de refus ou de non-réclamation du destinataire à compter de la date de son établissement. Et assurer à l'expéditeur l'accès, pendant au moins 1 an, aux informations relatives aux preuves de réception et preuves de refus ou de non-réclamation.

(articles 33.2.b et 39 de la loi 43-20 & articles 6,7 et 18 du décret 2.22.687) ;

(Critère 7) Garantir l'identification de l'expéditeur (et vérifier son identité) avec un degré de confiance élevé (article 28 de la loi 43-20 et article 5 du décret 2.22.687) ;

(Critère 8) Garantir l'identification du destinataire (et vérifier son identité) avant la fourniture des données (article 28 de la loi 43-20 et article 5 du décret 2.22.687) ;

(Critère 9) Assurer la sécurisation de l'envoi et de la réception des données objet de l'envoi recommandé, au travers d'une signature électronique avancée ou cachet électronique avancé, de manière à exclure toute possibilité de modification indétectable de ces données (article 28 de la loi 43-20) ;

(Critère 10) Assurer le signalement à l'expéditeur et au destinataire de toute modification des données nécessaire pour l'envoi ou la réception de celles-ci (article 28 de la loi 43-20) ;

(Critère 11) Utiliser un horodatage électronique qualifié pour indiquer la date et l'heure d'envoi, la date et l'heure de réception ainsi que toute modification des données (article 28 de la loi 43-20) ;

(Critère 12) Assurer l'établissement et la délivrance à l'expéditeur, dès réception (par le PSCo) des données objet de l'envoi recommandé, d'une preuve de dépôt contenant les informations spécifiées au niveau de l'article 6 du décret 2.22.687 (article 6 du décret 2.22.687) ;

(Critère 13) Garantir l'établissement d'une preuve de réception par le destinataire contenant les informations spécifiées au niveau de l'article 7 du décret 2.22.687 notamment la date et l'heure de l'envoi et de la réception, indiquées par un horodatage électronique qualifié (article 7 du décret 2.22.687) ;

(Critère 14) En cas de refus ou de non-réclamation par le destinataire : garantir l'établissement et la remise à l'expéditeur dans le délai convenu, d'une preuve de refus ou de non-réclamation par le destinataire, qui contient les informations spécifiées au niveau de l'article 7 du décret 2.22.687 notamment la date et l'heure du refus indiquées par un horodatage électronique qualifié (article 7 du décret 2.22.687).

A noter :

Le respect de ces critères de conformité se matérialise par la **mise en œuvre,** de la part du PSCo souhaitant fournir un service **d'envoi recommandé électronique qualifié,** des dispositions ci-dessous :

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

6 Exigences de conformité

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

Ref_Env_Reco_Qual_Exig 2. Le PSCo souhaitant fournir un service d'envoi recommandé électronique qualifié doit être agréé au sens de la loi 43-20 et son décret d'application. A ce titre, le PSCo doit impérativement se conformer aux exigences du référentiel **[Ref_PSCo_AG].**

6.1 Normes applicables

6.1.1 Norme ETSI 319 531 – Service QREMS

Cas spécifique = [si le service d'envoi recommandé électronique qualifié est un service d'envoi de courrier électronique recommandé qualifié] autrement dit, si le QERDS est un QREMS ;

Ref_Env_Reco_Qual_Exig 3. Les PSCo souhaitant fournir un **service d'envoi de courrier électronique recommandé qualifié** (QREMS) sont tenus de se conformer aux exigences de la norme **ETSI EN 319 531** v1.1.1 ou version ultérieure. Cela comprend :

- Dispositions générales autour des politiques et pratiques (chap. 4 – General provision on policies and practices) y inclut :
  - Déclaration des pratiques des services de courrier électronique recommandé (4.1 REMS Practice statement) ;
  - Conditions générales (4.2 Terms and conditions) ;
  - Politique de sécurité de l'information (4.3 Information security policy) ;
  - Nature des courriers électroniques recommandés (4.4 REM nature) ;
  - Modes de fonctionnement des courriers électroniques recommandés (4.5 REM styles of operation) ;
- Dispositions générales autour des courriers électroniques recommandés (chap. 5 – General provision on REMS) y inclut :
  - Intégrité et confidentialité des messages (5.1 Message integrity and confidentiality) ;
  - Identification et authentification des expéditeurs/destinataires (5.2 Sender and receiver identification and authentication) ;
  - Référence temporelle (5.3 Time reference) ;
  - Preuve (5.4 Evidence) ;
  - Interoperabilité (5.5 Interoperability) ;
- Evaluation de risques (chap. 6 –Risk assessments) ;
- Gestion et exploitation du prestataire de service d'envoi recommandé (chap. 7 – ERDSP management and operation) y inclut :
  - Organisation interne (7.1 Internal organization) ;
  - Ressources humaines (7.2 Human ressources) ;
  - Gestion des actifs (7.3 Asset management) ;

- Contrôle d'accès (7.4 Access control) ;
- Contrôle cryptographiques (7.5 Cryptographic controls) ;
- Sécurité physique et environnementale (7.6 Physical and environmental security) ;
- Sécurité de l'exploitation (7.7 Operation security) ;
- Sécurité réseau (7.8 Network security) ;
- Gestion des incidents (7.9 Incident management) ;
- Collecte de preuves (7.10 Collection of evidence for REMSP internal services) ;
- Gestion de la continuité d'activité (7.11 Business continuity management) ;
- Cessation d'activité du PSCo et plan associé (7.12 REMSP termination and REMS termination plans) ;
- Conformité (7.13 Compliance).

La norme ETSI 319 531 peut renvoyer vers d'autres normes ETSI ou vers l'ISO/IEC pour donner des orientations de mise en œuvre de certaines exigences.

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

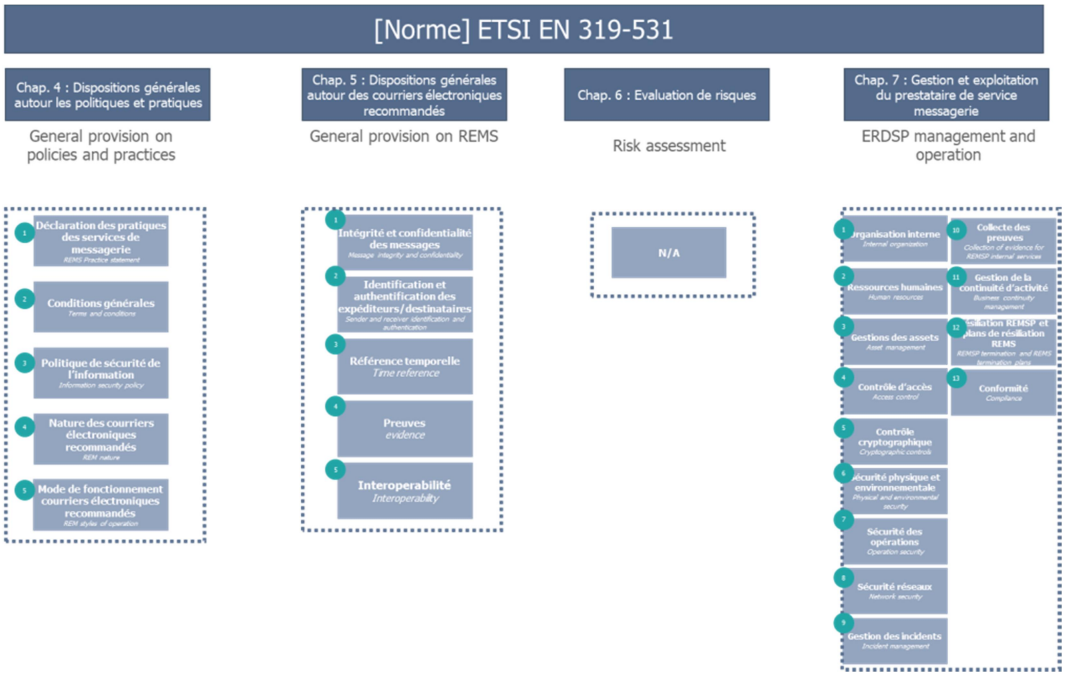

Figure 2 - Sujets couverts par la norme ETSI EN 319 531.

NB : cadre technique de mise en œuvre et interopérabilité

Afin de s'aligner avec les meilleures pratiques et permettre l'interopérabilité, il est recommandé de s'appuyer sur la norme ETSI EN 319 532 pour la mise en œuvre technique et protocolaire du service d'envoi de courrier électronique recommandé qualifié.

6.1.2 Norme ETSI 319 521 – Service QERDS

Cas général = [si le service d'envoi recommandé électronique qualifié n'est pas un service d'envoi de courrier électronique recommandé qualifié] autrement dit, si le QERDS n'est pas un QREMS.

Ref_Env_Reco_Qual_Exig 4. Les PSCo souhaitant fournir un service d'envoi recommandé électronique qualifié (QERDS autre que QREMS) sont tenus de se conformer aux exigences de la norme ETSI EN **319 521** version v1.1.1 ou ultérieure. Cela comprend :

- Les exigences relatives aux dispositions générales sur les politiques et pratiques (chap. 4 – General provision on policies and practices) y inclut :
  - *Déclaration des pratiques des prestataires de services d'envoi recommandé électronique (4.1 ERDSP Practice statement) ;*
  - *Conditions générales (4.2 Terms and conditions) ;*
  - *Politique relative à la sécurité de l'information (4.3 Information security policy) ;*
- Les dispositions générales relatives aux services d'envoi recommandé électronique (chap. 5 –General provision on ERDS) y inclut :
  - *Intégrité et confidentialité des données échangées (5.1 User content integrity and confidentiality) ;*
  - *Identification et authentification des utilisateurs (5.2 Users Identification and Authentication) ;*
  - *Référence temporelle (5.3 Time reference) ;*
  - *Evénements et preuves (5.4 Events and evidences) ;*
  - *Interopérabilité (5.5 Interoperability) ;*
- Evaluation des risques (chap. 6 –Risk assessments) ;
- Gestion et exploitation du prestataire de service d'envoi recommandé électronique (chap. 7 –ERDSP management and operation) y inclut :
  - *Organisation interne (7.1 Internal organization) ;*
  - *Ressources humaines (7.2 Human ressources) ;*
  - *Gestion des actifs (7.3 Asset management) ;*
  - *Contrôle d'accès (7.4 Access control) ;*
  - *Contrôle cryptographiques (7.5 Cryptographic controls) ;*
  - *Sécurité physique et environnementale (7.6 Physical and environmental security) ;*
  - *Sécurité de l'exploitation (7.7 Operation security) ;*
  - *Sécurité réseau (7.8 Network security) ;*
  - *Gestion des incidents (7.9 Incident management) ;*
  - *Collecte de preuves (7.10 Collection of evidence for ERDSP internal services) ;*
  - *Gestion de la continuité de service (7.11 Business continuity management) ;*
  - *Cessation d'activité du PSCo et plan associé (7.12 ERDSP termination and ERDS termination plans) ;*
  - *Conformité et exigences légales (7.13 Compliance and legal requirements) ;*

La norme ETSI 319 521 peut renvoyer vers d'autres normes ETSI ou vers l'ISO/IEC pour donner des orientations de mise en œuvre de certaines exigences.

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

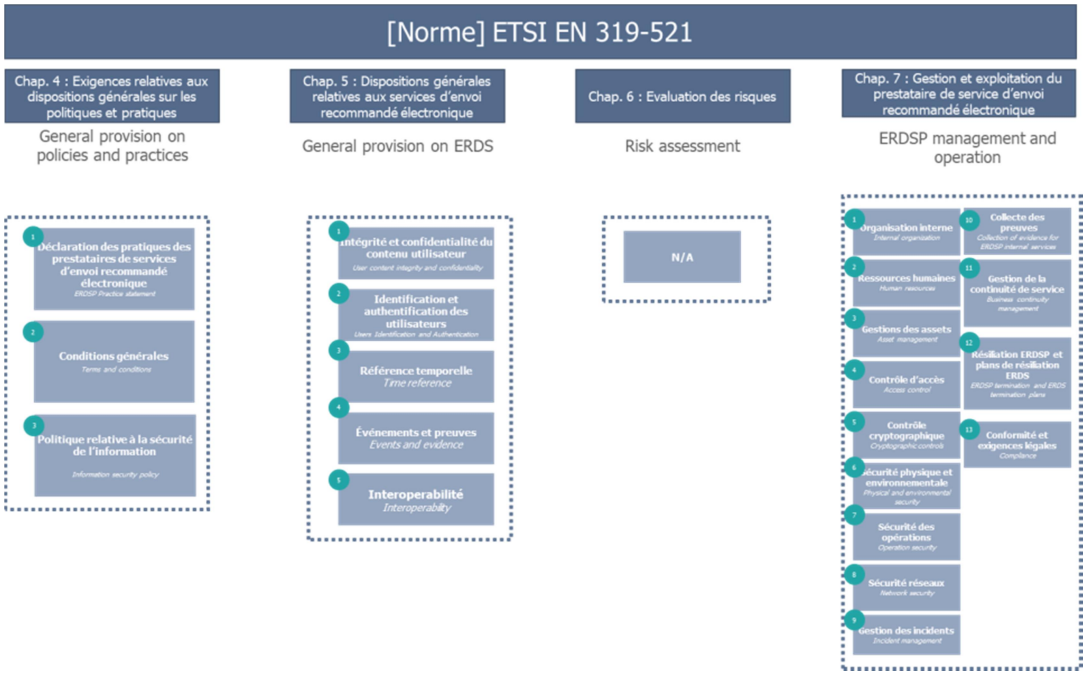

Figure 3 - Sujets couverts par la norme ETSI EN_319_521.

NB : cadre technique de mise en œuvre et interopérabilité

Afin de s'aligner avec les meilleures pratiques et permettre l'interopérabilité, il est recommandé de s'appuyer sur la norme ETSI EN 319 522 pour la mise en œuvre technique et protocolaire du service d'envoi recommandé électronique qualifié (autre que QREMS).

6.2 Compléments et précisions

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

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

L'ensemble de ces exigences complémentaires sont applicables indifféremment, aussi bien au cas général d'un QERDS qu'au cas spécifique d'un QREMS.

6.2.1 Identification de l'expéditeur et du destinataire

La vérification initiale de l'identité correspond à la vérification de l'identité réalisée avant (ou pendant) la 1ère utilisation du service pour chaque utilisateur du service (expéditeur ou destinataire). On parle de l'enrôlement de l'utilisateur qui devient ensuite connu du PSCo agréé (identité vérifiée et éventuellement moyens d'identification partagés permettant un accès sécurisé au services après une procédure d'authentification).

Ref_Env_Reco_Qual_Exig 5. La vérification initiale de l'identité de **l'expéditeur** (enrôlement) devra se faire conformément aux modalités relatives à la vérification initiale de l'identité au vu de la délivrance d'un certificat qualifié :

- A ce titre, le PSCo agréé devra mettre en œuvre un des schémas de vérification d'identité (schéma (a) ou (b) ou (c) ou (d)) définis au niveau du référentiel **[Ref_Deliv_Cert_Qual]**.

Ref_Env_Reco_Qual_Exig 6. La vérification initiale de l'identité du **destinataire** (enrôlement) doit se faire selon les modalités suivantes :

- Si le destinataire est une personne physique représentant une personne morale, ladite vérification initiale doit être réalisée selon les mêmes modalités que celles exigées pour la vérification initiale de l'identité de l'expéditeur ;
- Si le destinataire est une personne physique (ne représentant pas une personne morale), ladite vérification initiale doit être réalisée soit :
    - Selon les mêmes modalités que celles exigées pour la vérification initiale de l'identité de l'expéditeur ;

      Ou, à défaut
    - Suivant des modalités permettant de réduire considérablement le risque d'utilisation abusive ou d'altération de l'identité. Cela inclut nécessairement :
        - La collecte sécurisée et la vérification de l'authenticité de la carte nationale d'identité du destinataire (ou de tout autre document valide justifiant son identité comportant une photo d'identité et délivré par une autorité compétente) ;
        - L'établissement du lien entre le document d'identité présenté et la personne qui l'a présenté ;
        - La mise en place de mesures pour minimiser le risque que l'identité de la personne ne soit pas alléguée, en couvrant notamment les risques de perte, de vol, de suspension, de révocation ou d'expiration de la pièce d'identité.

Ref_Env_Reco_Qual_Exig 7. Postérieurement à la vérification initiale de l'identité de l'expéditeur et du destinataire, le PSCo agréé peut attribuer à chacun un moyen d'identification électronique qu'il pourra utiliser ensuite pour attester de son identité à chaque envoi ou réception ultérieurs.

Ces moyens doivent respecter les dispositions listées au niveau de la section 5.2.2 de la norme EN 319 521 (en particulier l'exigence REQ-QERDS-5.2.2-02). Cela implique notamment l'utilisation :

- De mécanismes d'authentification multi-facteurs, compatibles avec les bonnes pratiques de l'ISO 29115, faisant intervenir au moins 2 facteurs de natures différentes ;

  Et/Ou
- D'une signature électronique avancée conforme aux exigences de [Ref_Serv_Conf_NonQual] ;

Ref_Env_Reco_Qual_Exig 8. Si le PSCo agréé n'attribue pas de moyen d'identification à l'expéditeur ou au destinataire, la vérification de l'identité doit être réalisée à chaque envoi suivant les modalités de la vérification initiale de l'identité telle que spécifiée ci-dessus.

6.2.2 Fourniture du service par plusieurs PSCo agréés

Ref_Env_Reco_Qual_Exig 9. Conformément aux articles 28 et 32 de la Loi 43-20, lorsque le service d'envoi recommandé électronique qualifié est fourni par plusieurs PSCo, ils doivent obligatoirement être tous agréés au titre de la loi 43-20.

Ref_Env_Reco_Qual_Exig 10. Dans le cas où le service est fourni par plusieurs PSCo agréés, l'expéditeur et le destinataire de l'envoi recommandé électronique qualifié doivent être informés de l'identité de l'ensemble des PSCo agréés contribuant au service d'envoi recommandé électronique qualifié. Comme spécifié au chapitre 4.1.2 de la norme EN 319 421, la déclaration des pratiques du service d'envoi recommandé électronique qualifié (QERDS practice statement) doit absolument lister l'ensemble des PSCo agréés contribuant à la fourniture dudit service.

Ref_Env_Reco_Qual_Exig 11. Chaque PSCo agréé contribuant à la fourniture du service d'envoi recommandé électronique qualifié est responsable de s'assurer du maintien du statut agréé de ses PSCo partenaires contribuant à la fourniture dudit service, notamment en s'appuyant sur la liste nationale des PSCo agréés (LNPA) publiée par l'autorité nationale.

Ref_Env_Reco_Qual_Exig 12. Dans le cas où le PSCo agréé du service d'envoi recommandé électronique qualifié (PSCo du QERDS) s'appuie sur un PSCo agréé de service d'horodatage qualifié tiers, il (le PSCo du QERDS) devra systématiquement vérifier la validité du jeton d'horodatage électronique qualifié utilisé.

Ref_Env_Reco_Qual_Exig 13. Dans le cas où le PSCo agréé du service d'envoi recommandé électronique qualifié (PSCo du QERDS) s'appuie sur un PSCo agréé tiers pour le cachet électronique avancé (ou la signature électronique avancée) sécurisant l'envoi et la réception des données, il (le PSCo du QERDS) devra systématiquement vérifier la validité du cachet (ou de la signature) utilisé(e).

6.2.3 Preuves concernant le traitement des données transmises

Ref_Env_Reco_Qual_Exig 14. Conformément à l'article 27 de loi 43-20 et aux articles 6 et 7 du décret 2.22.687, le PSCo devra mettre à disposition de l'expéditeur a minima les preuves suivantes :

- La preuve de dépôt *par l'expéditeur* : délivrée à l'expéditeur dès réception par le PSCo agréé des données (objet de l'envoi recommandé) à transmettre au destinataire de la part de l'expéditeur. Elle contient a minima les informations spécifiées au niveau de l'article 6 du décret 2.22.687 ;

  Cette preuve de dépôt adresse « la preuve d'envoi par l'expéditeur » prévue au niveau de l'article 27 de la loi 43-20.

- La preuve de réception *par le destinataire* : délivrée à (mise à disposition de) l'expéditeur dès réception des données par le destinataire. Elle contient les informations spécifiées au niveau de l'article 7 du décret 2.22.687 notamment la date et l'heure de l'envoi et de la réception, indiquées par un horodatage électronique qualifié ;

- La preuve de refus ou de non-réclamation *par le destinataire* : délivrée à (mise à disposition de) l'expéditeur en cas de refus ou de non-réclamation par le destinataire, dans le délai convenu entre le PSCo agréé et l'expéditeur. Elle contient les informations spécifiées au niveau de l'article 7 du décret 2.22.687 notamment la date et l'heure du refus indiquées par un horodatage électronique qualifié.

Ref_Env_Reco_Qual_Exig 15. Le PSCo agréé doit garantir à l'expéditeur un accès automatisé, fiable, et sécurisé, à ces différentes preuves. Les conditions générales d'utilisation du service d'envoi recommandé électronique qualifié doivent préciser les modalités de mise à disposition et d'accès à ces preuves.

6.2.4 Sécurisation et horodatage des échanges

Ref_Env_Reco_Qual_Exig 16. Conformément à l'article 28 du décret 2.22.687 et aux dispositions du paragraphe 5.1.2 de la norme 319 521, l'envoi et la réception de données objet de l'envoi recommandé qualifié QERDS, doivent être sécurisés a minima par un cachet électronique avancé (ou une signature électronique avancée) dont la validité a été vérifié(e) et qui a été généré(e) un PSCo agréé.

Il est recommandé que le certificat sur lequel repose ce cachet électronique avancée (ou cette signature électronique avancée) soit un certificat qualifié au titre de la loi 43-20 et conformément aux exigences de [Ref_Deliv_Cert_Qual].

Ref_Env_Reco_Qual_Exig 17. Conformément à l'article 28 du décret 2.22.687 et aux dispositions du paragraphe 5.3.2 de la norme 319 521, la date et l'heure d'envoi et de réception ainsi que toute modification des données doivent être indiquées par un horodatage électronique qualifié.

6.2.5 Signalement des modifications de données

Ref_Env_Reco_Qual_Exig 18. Conformément au point (5) de l'article 28 de la loi 43-20, le service QERDS doit signaler clairement à l'expéditeur et au destinataire toute modification des données nécessaire pour l'envoi ou la réception de celles-ci :

- Le PSCo agréé doit préciser dans les conditions générales d'utilisation du service QERS les moyens utilisés pour le signalement de ces modifications ;
- Les moyens mis en œuvre doivent permettre la réalisation de ce signalement dans les plus brefs délais dès l'occurrence de la modification.

6.2.6 Conservation des données

[Précisions relatives aux dispositions des articles 6,7 et 18 du décret 2.22.687].

En complément aux exigences du référentiel [Ref_PSCo_AG] et aux exigences des normes EN 319 521 et EN 319 531.

Ref_Env_Reco_Qual_Exig 19. Conformément aux articles 6 et 7 du décret 2.22.687, la preuve de dépôt, la preuve de réception et le cas échéant la preuve de refus ou de non-réclamation du destinataire doivent être conservés pendant **une durée minimale de un (1) an** à compter de la date d'établissement de ladite preuve.

Ref_Env_Reco_Qual_Exig 20. Conformément à l'article 18 du décret n° 2.22.687, le PSCo agréé de service d'envoi recommandé électronique qualifié est tenu de conserver pendant une **durée minimale de sept (7) ans,** après la date d'envoi et de réception des données, toutes les informations pertinentes concernant les données délivrées et reçues, notamment afin de pouvoir assurer le service et le cas échéant fournir des preuves suffisantes en cas de litige.

Ref_Env_Reco_Qual_Exig 21. Concernant les données à conserver par le PSCo agréé de service d'envoi recommandé électronique qualifié, les dispositions de la norme ETSI EN 319 521 (notamment REQ-ERDS-5.4.1-03) s'appliquent. Les données à conserver sont au moins :

- L'identité de l'expéditeur du recommandé électronique ;
- Une preuve de validation de l'identité de l'expéditeur ;
- L'identité du destinataire du recommandé électronique ;
- Une preuve de validation de l'identité du destinataire ;
- Une référence (ou un condensé) aux (des) données faisant l'objet de la demande d'envoi recommandé électronique ;
- Les journaux (logs) des événements/opérations du service (notamment les logs relatifs aux opérations de vérification de l'identité de l'expéditeur et du destinataire et les logs des échanges) ;
- Les jetons d'horodatage électronique qualifiés correspondant à la date et heure d'envoi, de réception et de modification des données le cas échéant ;
- Les données relatives à la sécurisation de l'envoi (cachets électroniques ou signatures électroniques).

6.2.7 Modules cryptographiques utilisés

Ref_Env_Reco_Qual_Exig 22. Les modules cryptographiques utilisés pour les opérations nécessaires au service d'envoi recommandé électronique qualifié, notamment les opérations listées ci-dessous, doivent être conformes aux dispositions relatives aux modules cryptographiques spécifiées au niveau du référentiel **[Ref_PSCo_AG]** :

- Création du cachet ou de la signature électronique sécurisant l'envoi et la réception des données ;

- Génération des certificats et/ou la génération des clés privées de signature ou de cachet ;
- Horodatage électronique qualifié.

6.2.8 Publication sur la liste nationale des PSCo agréés

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

Ref_Env_Reco_Qual_Exig 23. L'identification d'un service d'envoi recommandé électronique qualifié dans la Liste Nationale des PSCo Agréés (LNPA) doit respecter les exigences définies dans [Ref_PSCo_AG].

Ref_Env_Reco_Qual_Exig 24. L'identification d'un service d'envoi recommandé électronique qualifié dans la Liste Nationale des PSCo Agréés (LNPA) se fait :

- Soit au moyen du certificat électronique utilisé pour apposer le cachet électronique avancé (ou la signature électronique avancée) permettant de sécuriser l'envoi et la réception des données :
    - Dans ce cas, si plusieurs certificats de cachet électronique (et/ou de signature) sont mis en oeuvre pour un même service d'envoi recommandé électronique qualifié, cela donne lieu à l'inscription de plusieurs services dans la liste de confiance ;
- Soit au moyen du certificat électronique d'une autorité de certification (AC) opérée sous la responsabilité du PSCo agréé et qui satisfait les 2 conditions suivantes :
    (1) L'AC ne délivre des certificats qu'à l'attention exclusive de services de confiance opérés par le PSCo agréé ;
    (2) L'AC ne délivre pas de certificats pour des services d'envoi recommandé électronique non qualifiés (autrement dit, les services d'envoi recommandé électronique non qualifiés ne font pas partie des services de confiance opérés par le PSCo agréé sous l'AC en question) ;
    - Dans ce cas, le PSCo agréé doit pouvoir démontrer le respect des conditions (1) et (2) et la mise en place de mesures organisationnelles et techniques appropriées afin d'assurer le maintien du respect de ces 2 conditions dans la durée.

7 Annexes

Liens vers les normes et standards

- **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_319521v010101p.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_319531v010101p.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