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

[Ref_QSCD]

Exigences de conformité relatives aux

Dispositifs qualifiés de création de signature ou de cachet électronique

Suivi des mises à jour du document [Ref_QSCD]

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

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

PSCo-dsr@dgssi.gov.ma

Sommaire

1 Terminologie et acronymes

Autorité nationale : fait référence à l'autorité nationale des services de confiance pour les transactions électroniques au sens du décret n° 2.22.687 pris pour l'application de la loi n°43-20 relative aux services de confiance pour les transactions électroniques, à savoir la Direction Générale de la Sécurité des Systèmes d'Information (DGSSI) relevant de l'Administration de la défense nationale.

QSCD *(Qualified Signature/Seal Creation Device)* : désigne un dispositif qualifié de création de signature électronique ou de cachet électronique au sens de la loi n° 43-20.

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

PSCo agréé : désigne un prestataire de service de confiance agréé (ou souhaitant se faire agréer) au sens de la Loi n° 43-20.

CC : Common Criteria for Information Technology Security Evaluation.

HSM *(Hardware Security Module)* : périphérique physique sécurisé en mesure de générer, protéger et gérer les clés cryptographiques utilisées pour les opérations telles que le chiffrement, le déchiffrement et la création des signatures électroniques et de certificats électroniques en toute sécurité.

Profil de protection (PP) : document public qui définit, pour une catégorie de produits, un ensemble d'exigences et d'objectifs de sécurité, indépendants de leur technologie et de leur implémentation, qui satisfont les besoins de sécurité communs à un groupe d'utilisateurs ou à un cas d'usage.

CEN : Comité Européen de Normalisation (CEN).

ETSI : European Telecommunications Standards Institute (ETSI).

2 Objet et périmètre

Le présent document, désigné par **[Ref_QSCD],** constitue le référentiel fixant les exigences de conformité pour les dispositifs qualifiés de création de signature électronique au sens de l'article 8 de la loi n° 43-20 et du cachet électronique au sens de l'article 17 de ladite loi n° 43-20.

La loi n° 43-20 dispose que pour créer une signature électronique qualifiée ou un cachet électronique qualifié, le dispositif de création de signature électronique ou de cachet électronique doit lui-même être qualifié.

La conformité de ces dispositifs aux exigences de la loi n° 43-20 et de ses textes pris pour son application est attestée par un certificat de conformité délivré par la DGSSI.

3 Modalités de mise à jour

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

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

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

4 Cadre de référence

4.1 Cadre juridique et normatif

Le cadre légal de référence sur lequel repose **[Ref_QSCD]** 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), en particulier les articles du Chapitre I / Section I **« Des services de confiance »** .
- Les dispositions du **décret n° 2.22.687** pris pour l'application de la loi n°43-20 en particulier le chapitre Premier / Section 2 relative aux modalités de délivrance des certificats de conformité.

Les normes et standards suivants :

- Les critères communs (CC) :
  - ISO/IEC 15408-1:2009 — Technologies de l'information — Techniques de sécurité — Critères d'évaluation pour la sécurité TI — Partie 1. ISO, 2009 ;
  - ISO/IEC 15408-2:2008 — Technologies de l'information — Techniques de sécurité — Critères d'évaluation pour la sécurité TI — Partie 2. ISO, 2008 ;
  - ISO/IEC 15408-3:2008 — Technologies de l'information — Techniques de sécurité — Critères d'évaluation pour la sécurité TI — Partie 3. ISO, 2008 ;

    et
  - ISO/IEC 18045:2008 — Technologies de l'information — Techniques de sécurité — Méthodologie pour l'évaluation de sécurité TI.

- Les profils de protection (PP) pour dispositif sécurisé de création de signature électronique — CEN EN 419 211 Parties 1 à 6 (applicable à la création de signature électronique dans un environnement dont l'utilisateur a la gestion totale) :
  - EN 419 211-1:2014 — Profils de protection pour dispositif sécurisé de création de signature électronique — Partie 1: Présentation générale,
  - EN 419 211-2:2013 — Profils de protection des dispositifs sécurisés de création de signature — Partie 2: Dispositif avec génération de clé,
  - EN 419 211-3:2013 — Profils de protection des dispositifs sécurisés de création de signature — Partie 3: Dispositif avec import de clé,
  - EN 419 211-4:2013 — Profils de protection des dispositifs sécurisés de création de signature — Partie 4: Extension pour un dispositif avec génération de clé et communication sécurisée avec l'application de génération de certificats,
  - EN 419 211-5:2013 — Profils de protection des dispositifs sécurisés de création de signature — Partie 5: Extension pour un dispositif avec génération de clé et communication sécurisée avec l'application de création de signature,
  - EN 419 211-6:2014 — Profils de protection pour dispositif sécurisé de création de signature électronique — Partie 6: Extension pour un dispositif avec import de clé et communication sécurisée avec l'application de création de signature.

- Cas de dispositifs qualifiés de création de signature/cachet électronique, lorsqu'un PSCo agréé gère les données de création de signature/cachet électronique pour le compte d'un signataire ou d'un créateur de cachet :
  - **CEN EN 419 221-5** « Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services » ;

- **CEN EN 419 241 -1** Trustworthy Systems Supporting Server Signing — Part 1: General System Security Requirements ;
- **CEN EN 419 241 -2** Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing.

➢ Algorithmes et mécanismes cryptographiques :

- **[Standard] ETSI TS 119 312 :** Electronic Signatures and Infrastructures (ESI); Cryptographic Suites ;

Figure 1 : Structure du cadre juridique et normatif

4.2 Précaution d'interprétation des normes et standards ETSI

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

L'utilisation de ce cadre présente un double avantage :

➢ Garantir la fiabilité, la sécurité, la pérennité et la robustesse des services de confiance fournis au niveau national ;

➢ Permettre la reconnaissance à l'international des services fournis par les PSCo établis au niveau national et faciliter les échanges électroniques avec les pays partenaires.

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

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

- Les références au cadre réglementaire Européen « Directive 95/46/EC » « Regulation (EU) No 910/2014 » et aux chapitres et articles associés, doivent être replacées et interprétées dans le contexte national.
  - ➢ Le cadre réglementaire à prendre en compte est bien le cadre national à savoir la **« Loi 43-20 »** et son **« Décret d'application n° 2.22.687 »** tel que rappelé dans

ce document **;**

- Les dispositions, articles et chapitres concernant la prestation ou le service de confiance objet du référentiel sont rappelés dans le corps de chaque référentiel ;

- Le terme **« EU qualified »** est à transposer en **:**
  - **« Agréé »** lorsqu'il s'agit d'un **PSCo ;**
  - **« Qualifié »** lorsqu'il s'agit d'un **service de confiance ;**
- Les « **EU official languages** » (langues officielles européennes) à considérer dans le contexte national sont **l'anglais** et/ou le **français** ;
- Comme précisé par l'ETSI, les termes « s**hall / shall not** » indiquent des **exigences obligatoires** qui doivent être **strictement respectées** et **mises en œuvre** par le PSCo :
  - Plus largement, les verbes modaux et auxiliaires utilisés dans les différentes normes ETSI sont à interpréter conformément aux indications de la clause 3.2 de **l'ETSI Drafting Rules ;**
- En cas de doute concernant une référence très spécifique à l'Union Européenne, jugée non applicable dans le contexte national ➔ se rapprocher de l'autorité nationale.

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

Les principaux articles et dispositions de la loi n° 43-20 applicables spécifiquement aux dispositifs qualifiés de création de signature ou de cachet électronique, sont consolidés au niveau du tableau suivant :

Titre préliminaire Dispositions générales	**Article 2**	Définition du dispositif de création de signature/cachet électronique au sens de la loi.
Chapitre Ier Section Ière Des services de confiances	**Article 6**	Conditions à respecter pour créer une signature électronique qualifiée.
	Article 8	Exigences applicables aux dispositifs qualifiés de création de signature électronique.
	Article 17	Exigences applicables aux dispositifs qualifiés de création de cachet électronique.
Chapitre Ier Section Ière Des services de confiances Section III	**Article 41**	Responsabilités du titulaire de certificat électronique en matière de confidentialité de de l'intégrité des données afférentes à la création de la signature/cachet électronique qualifié lorsque ces données se trouvent dans un dispositif qualifié de création de signature /cachet électronique.

Tableau 1: *Récapitulatif des principaux articles et dispositions de la loi n°43-20 relatifs aux QSCD.*

4.4 Rappel des principales dispositions du décret n° 2.22.687 applicables

Les principaux articles et dispositions du décret n° 2.22.687 applicables spécifiquement aux dispositifs qualifiés de création de signature et de cachet électronique, sont consolidés au niveau du tableau suivant :

Chapitre Ier Section II « Des modalités de délivrance des certificats de conformité»	**Article 8**	Constituants du dossier de demande du certificat de conformité (Annexe n°1) ; Obligation de notification en cas de modification durant la période d'examen.
	Article 9	Durée de validité du certificat de conformité, qui ne peut pas excéder 5 ans. Mise à jour de la liste des dispositifs qualifiés de création de signature/cachet électronique.
	Article 10	L'obligation d'informer la DGSSI toute modification ou évolution concernant le dispositif avec la fourniture d'un rapport d'analyse de risques et d'impacts.
	Article 11	Modalités de renouvellement du certificat de conformité.
	Article 12	Modalités de suspension ou de retrait du certificat de conformité.

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

5 Procédure de délivrance du certificat de conformité

5.1 Modalités de dépôt et d'envoi du dossier de la demande

Les modalités relatives à la demande du certificat de conformité sont précisées au niveau de l'article 8 du décret n° 2.22.687, à savoir :

- Dépôt physique du dossier de la demande auprès de l'autorité nationale ou envoi recommandé du dossier (envoi postal ou électronique),
  - Le formulaire de la demande, 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 ladite demande sont précisés au niveau de l'annexe n° 1 du décret n° 2.22.687.
  - Un récépissé de réception de la demande est remis au demandeur.
- Communication à l'autorité nationale par le demandeur, de toute modification éventuelle affectant un des éléments de la demande,
  - Transmission des documents mis à jour en tenant compte des modifications survenues.

5.2 Forme du certificat de conformité

Le certificat de conformité porte mention des fonctions pour lesquelles il a été délivré et du rapport de certification relatif au certificat de sécurité (CC) sur lequel il s'appuie, ainsi que sa durée de validité. Ce certificat de conformité peut comporter des restrictions d'usage qui doivent impérativement être respectées, notamment dans le cadre de la préparation, de la délivrance puis de la mise en œuvre du dispositif.

Dans le cas de la certification de conformité du QSCD utilisés dans l'environnement d'un prestataire de services de confiance agréé, assurant la génération et la gestion des données de création de signature (respectivement de cachet) pour le compte du signataire (respectivement du créateur de cachet), un certificat de conformité partiel peut être délivré pour le seul produit. Ce certificat de conformité devra être complété après la vérification des modalités de mise en œuvre du QSCD dans l'environnement d'un prestataire de services de confiance agréé.

5.3 Validité du certificat de conformité

Etant donné que Le certificat de conformité est lié au certificat de sécurité (CC), ce certificat CC doit rentrer dans un processus de surveillance. Le certificat de surveillance est attendu par l'autorité nationale dans un délai maximal de 5 ans après la décision de certification (CC) ou la dernière surveillance et ce, afin de permettre le maintien du certificat de conformité en question.

Le certificat de conformité est délivré pour une version identifiée du QSCD, et son durée de validité est mentionnée dans ledit certificat. Dans tous les cas, la durée de validité du certificat de conformité ne peut dépasser 10 ans au-delà de la certification (CC) ou de la dernière surveillance du QSCD en question.

5.4 Maintenance du certificat de conformité

Toute nouvelle version doit faire l'objet d'une décision explicite d'extension du certificat de conformité, dans les mêmes conditions que la décision initiale d'attribution du certificat de conformité.

Une fois la décision de certification de conformité arrivée à échéance ou révoquée, le QSCD est retiré de la liste publiée par l'autorité nationale.

5.5 Critères de conformité

En vue de l'obtention du certificat de conformité, le demandeur 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 des textes pris pour son application :

Garantir par des moyens techniques et des procédures appropriés, que :

Critère 1	Les données de création de signature/cachet électronique utilisées pour créer la signature/cachet électronique ne peuvent être trouvées par déduction et que la signature/cachet électronique est protégée de manière fiable contre toute falsification par les moyens techniques actuellement disponibles
Critère 2	Les données de création de signature/cachet électronique utilisées pour créer la signature/cachet électronique ne peuvent être pratiquement établies qu'une seule fois ;
Critère 3	La confidentialité des données de création de signature/cachet électronique utilisées pour créer la signature/cachet électronique est assurée
Critère 4	Les données de création de signature/cachet électronique utilisées pour créer la signature/cachet électronique peuvent être protégées de manière fiable et satisfaisante par le signataire/créateur du cachet légitime contre toute utilisation par des tiers.

Et :

Critère 5	Les dispositifs qualifiés de création de signature/cachet électronique n'entraine aucune modification ou altération du contenu à signer/cacheter et n'empêchent pas la présentation de ce contenu au signataire/créateur du cachet avant la signature/le cachet.
Critère 6	La génération ou la gestion de données de création de signature/cachet électronique pour le compte du signataire/créateur du cachet peut être seulement confiée à un prestataire de services de confiance **agréé**.

A noter

Le respect de ces critères de conformité, au vu de la délivrance du certificat de conformité, se matérialise par la **mise en œuvre** de la part du demandeur des dispositions précisées dans le chapitre ci-dessous « **Exigences de conformité** »

6 Exigences de conformité

Les exigences de sécurité et leurs spécifications de certification respectives sont différentes :

- Lorsque le signataire/créateur du cachet possède matériellement un produit (Type 1) ;
- Lorsqu'un PSCO **agréé** gère les données de création de signature ou de cachet électronique pour le compte du signataire/créateur du cachet (Type 2).

6.1 Cas Type 1

Le Type 1 concerne les QSCD pour lesquels les données de création de signature ou de cachet électronique sont conservées dans un environnement sous le contrôle total de l'utilisateur, typiquement lorsque le signataire/créateur du cachet possède matériellement un produit.

Ref_QSCD_Exig 1. Dans ce cas, la certification de conformité par la DGSSI repose sur les normes référencées dans l'annexe I du présent référentiel. Le QSCD doit être **certifié conforme** selon ces normes.

6.2 Cas Type 2

Le Type 2 concerne les QSCD pour lesquels les données de création de signature ou de cachet électronique sont gérées par un prestataire de services de confiance agréé pour le compte du signataire ou du créateur de cachet.

Dans ce cas, la certification de conformité du QSCD (Type 2) ne peut se faire en dehors de l'évaluation du contexte d'exécution des opérations relatives à la création de la signature/cachet électronique qualifié.

L'évaluation en vue de la délivrance du certificat de conformité doit donc couvrir :

- Le **module cryptographique** (typiquement le HSM) sur lequel se base le QSCD
- **L'enchaînement sécurisé**, de bout en bout, **des opérations** relatives à la création et/ou à la gestion des données de création de signature/cachet électronique qualifié.
    - Cela implique que les **systèmes, mis en œuvre** pour la réalisation de cet enchaînement d'opérations, doivent garantir un niveau de confiance similaire à celui du module cryptographique lui-même, avec les certifications correspondantes (cf. plus bas)
- **L'environnement global** d'exécution et les **pratiques de gestion opérationnelle et de gouvernance** associées
    - Cela implique, conformément aux articles 8 et 9 de la loi n° 43-20, que le PSCo soit un PSCo agréé au sens de ladite loi n° 43-20.

Le respect des dispositions de l'exigence Ref_QSCD_Exig2. ci-après, permet d'adresser ces différents points.

Ref_QSCD_Exig 2. Dans le cas du Type 2, la certification de conformité est conditionnée par le respect des conditions ci-après :

(2.1) Le PSCo qui génère ou qui opère les données de création de signature/cachet électronique qualifiée pour le compte du signataire ou créateur du cachet, doit être obligatoirement un PSCo **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].**

(2.2) Le respect des dispositions du **chapitre 7 « Cas de la création de signature électronique qualifiée à distance »** du référentiel **[Ref_Deliv_Cert_Qual]** relatif aux exigences de conformité des prestataires fournissant des services de délivrance de certificats électroniques qualifiés. Cela implique notamment le respect des normes :

- **CEN EN 419 221-5** « Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services » ;
- **CEN EN 419 241 -1** Trustworthy Systems Supporting Server Signing — Part 1: General System Security Requirements ;
- **CEN EN 419 241 -2** Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing ;
- Le niveau 2 de garantie de contrôle exclusif (**SCAL2**) précisées au niveau des normes **EN 419 241-1** et **EN 419 241-1-2** ;

*Les dispositions de cette exigence (2.2) s'applique mutadis mutandis à la création de cachet électronique qualifié***.**

(2.3) Assurer la confidentialité de la clé privée de l'utilisateur (signataire/créateur du cachet), à tout moment depuis sa génération jusqu'à sa destruction.

Le respect des dispositions du point 2.2 doit être **attesté par une certification démontrant la conformité** par rapport aux normes CEN indiquées dans ce point.

Annexes I

Liste des normes applicables aux QSCD de Type 1

Les normes et standards applicables aux QSCD de Type 1 sont les suivants :

- Les critères communs (CC) :
  - ISO/IEC 15408-1:2009 — Technologies de l'information — Techniques de sécurité — Critères d'évaluation pour la sécurité TI — Partie 1. ISO, 2009 ;
  - ISO/IEC 15408-2:2008 — Technologies de l'information — Techniques de sécurité — Critères d'évaluation pour la sécurité TI — Partie 2. ISO, 2008 ;
  - ISO/IEC 15408-3:2008 — Technologies de l'information — Techniques de sécurité — Critères d'évaluation pour la sécurité TI — Partie 3. ISO, 2008 ;

    et
  - ISO/IEC 18045:2008 — Technologies de l'information — Techniques de sécurité — Méthodologie pour l'évaluation de sécurité TI.

- Les profils de protection (PP) pour dispositif sécurisé de création de signature électronique — CEN EN 419 211 Parties 1 à 6 :
  - EN 419 211-1:2014 — Profils de protection pour dispositif sécurisé de création de signature électronique — Partie 1: Présentation générale,
  - EN 419 211-2:2013 — Profils de protection des dispositifs sécurisés de création de signature — Partie 2: Dispositif avec génération de clé,
  - EN 419 211-3:2013 — Profils de protection des dispositifs sécurisés de création de signature — Partie 3: Dispositif avec import de clé,
  - EN 419 211-4:2013 — Profils de protection des dispositifs sécurisés de création de signature — Partie 4: Extension pour un dispositif avec génération de clé et communication sécurisée avec l'application de génération de certificats,
  - EN 419 211-5:2013 — Profils de protection des dispositifs sécurisés de création de signature — Partie 5: Extension pour un dispositif avec génération de clé et communication sécurisée avec l'application de création de signature,
  - EN 419 211-6:2014 — Profils de protection pour dispositif sécurisé de création de signature électronique — Partie 6: Extension pour un dispositif avec import de clé et communication sécurisée avec l'application de création de signature.
- Algorithmes et mécanismes cryptographiques :
  - Les algorithmes et mécanismes cryptographiques mis en œuvre par le QSCD doivent être conformes aux spécifications définies au niveau de la norme ETSI TS 119 312 V1.4.2 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.

*** Les parties 5 et 6 de la norme EN 419 211 fournissent des extensions relatives à l'environnement pour des dispositifs qualifiés de création de signature électronique, comme la communication avec des applications de création de signature de confiance. Bien que leur adoption soit fortement recommandée, les fabricants de produits sont libres d'appliquer ces extensions. La certification ne devrait pas s'étendre au-delà de la protection des données de création de signature électronique, et les applications de création de signature électronique ne sont pas couvertes par la certification.

Annexes II

Liens vers les normes et standard

- CC : Common criteria for Information Technology Security Evaluation
  - **www.commoncriteriaportal.org/cc/**

- Lien officiel vers les normes CEN 419 xxx :
  - **https://www.en-standard.eu/csn-standards/36-electrical-engineering/3698-processing-and-interchange-of-documents/**

- **ETSI TS 119 312** Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
  - **Se référer à la version la plus récente** publiée sur le site de l'ETSI : **https://www.etsi.org/deliver/etsi_ts/119300_119399/119312/**
  - A titre indicatif, la version la plus récente au moment de la rédaction du présent document est la suivante (v1.4.2) **https://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.04.02_60/ts_119312v010402p.pdf**

- **ETSI Drafting Rules** : règles d'interprétation des verbes modaux et auxiliaires utilisés au niveau des exigences des normes et standard ETSI
  - **https://docbox.etsi.org/stf/archive/STF473_SatEC_MAMES/STFworkarea/DraftDeliverables/background%20material/ETSI%20Drafting%20Rules%20%5Bexcerpt%20from%2033_directives_may_2014%5D%2BJRmarking.pdf**