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

Loi n° 43-20 relative aux services de confiance pour les transactions électroniques

-Foire aux questions-

2023

INFORMATIONS

PERSONNES AYANT CONTRIBUÉ À LA RÉDACTION DE CE DOCUMENT :

Rédigé par	Version	Date
DGSSI	1.0	01/01/2023

ÉVOLUTION DU DOCUMENT :

Version	Date	Nature des modifications
1.0	01/01/2023	Version initiale
1.1	13/07/2023	-Entrée en vigueur de la loi 43-20 -Publication des référentiels d'exigences

PUBLIC CONCERNÉ PAR CE DOCUMENT :

Tout public

POUR TOUTE REMARQUE :

Contact	Email
DGSSI /DSR	contact-dsr@dgssi.gov.ma

*Pour toute question, observation ou suggestion concernant ce document, veuillez-vous adresser à : **contact-dsr@dgssi.gov.ma***

Sommaire

I. INTRODUCTION

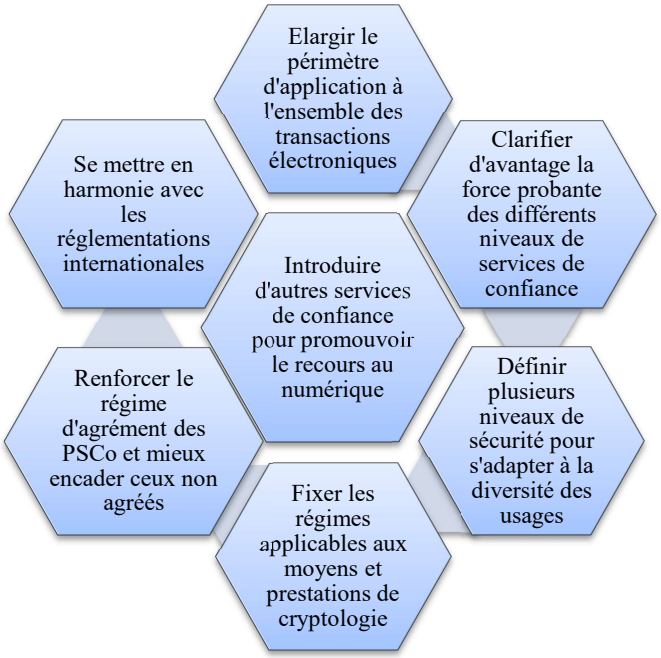
Au regard des évolutions réglementaires et technologiques dans le domaine de la confiance numérique, et compte tenu de la diversité des usages et des besoins métiers croissants engendrés par la transformation numérique que connait notre pays, le besoin de refonte de la loi n° 53.05 relative à l'échange électronique de données juridiques s'est fait fortement ressentir. C'est dans ce cadre que s'inscrit l'avènement de la loi n°43-20 relative aux services de confiance pour les transactions électroniques, applicable depuis le 13 juillet 2013.

L'objectif de ce document est d'éclairer les utilisateurs et les différents acteurs intervenant dans le domaine de la confiance numérique sur les questions relatives au cadre régissant les services de confiance au Maroc, afin de favoriser une compréhension commune et partagée par toutes les parties prenantes.

II. QUESTIONS RELATIVES A L'ENSEMBLE DES SERVICES DE CONFIANCE

1. Quels sont les principaux objectifs de la loi n° 43-20 ?

Les principaux objectifs de la loi n° 43-20 se présentent comme suit :



2. Quels sont les textes d'application de la loi n° 43-20 ?

Le seul texte d'application relatif aux services de confiance publié à la date de la rédaction du présent document est le décret n° 2.22.687 pris pour l'application de la loi n° 43-20 relative aux services de confiance pour les transactions électroniques.

Pour ses aspects techniques, le cadre juridique de la loi n° 43-20 renvoie à des référentiels d'exigences relatifs aux services de confiance, qui sont publiés sur le site Internet de l'autorité nationale (DGSSI[1]).Ces référentiels fixent les normes et les règles de sécurité applicables aux PSCo [2]et aux services qu'ils fournissent.

[1] Direction générale de la sécurité des systèmes d'information relevant de l'Administration de la Défense Nationale.

[2] Prestataire de services de confiance

3. Que devient loi n° 53-05 et ses textes d'application suite à l'entrée en vigueur de la loi n° 43-20 ?

La loi n° 43-20 abroge le chapitre premier et le titre II de la loi n° 53-05 relative à l'échange électronique de données juridiques, tandis que le titre premier relatif à la validité des actes sous forme électronique ou transmis par voie électronique et qui introduit la signature électronique dans le Dahir formant code des obligations et des contrats (DOC) demeure en vigueur.

La loi n° 43-20 prévoit des mesures transitoires pour (i) les prestataires de certification électronique (PSCE) agréés au titre de la loi n° 53-05, pour (ii) les certificats électroniques sécurisés, et pour (iii) les dispositifs de création de signature électronique attestés par un certificat de conformité délivrés conformément aux dispositions de la loi n° 53-05.

4. Quels sont les apports du volet « services de confiance » de la loi n° 43-20 ?

La loi n° 43-20 instaure un cadre juridique général pour l'utilisation des services de confiance. Elle étend le champ d'application de l'ancienne loi n° 53.05 relative à l'échange électronique de données juridiques au-delà de la seule signature électronique et englobe les services suivants :

- *La création de signatures électroniques, de cachets électroniques, d'horodatage électronique et d'envoi recommandé électronique ;*
- *La création des certificats électroniques relatifs aux signatures électroniques, aux cachets électroniques ou à l'authentification des sites internet ;*
- *La validation des signatures électroniques ou des cachets électroniques ;*
- *La conservation des signatures électroniques et des cachets électroniques ou des certificats relatifs à ces services.*

5. Quels sont les effets juridiques de la loi n° 43-20 ?

Conformément à la loi n° 43-20, l'effet juridique et la recevabilité comme preuve en justice des signatures électroniques, des cachets électroniques, des horodatages électroniques, et des envois recommandés électroniques, ne peuvent être refusés au seul motif que ces derniers se présentent sous forme électronique ou qu'ils ne sont pas qualifiés.

Par exemple, lorsque le procédé de signature électronique n'est pas qualifié, alors sa fiabilité devra être démontrée. L'acte signé n'est pas suffisant pour démontrer le consentement des parties à son contenu. Pour que la signature électronique non qualifiée ait la même valeur juridique qu'une signature manuscrite, il faudra apporter la preuve de sa fiabilité grâce à un dossier de preuve décrivant le procédé de signature utilisé et les procédés techniques assurant sa fiabilité.

Pour le niveau qualifié, la loi n° 43-20 précise les effets juridiques suivants :

- *La signature électronique qualifiée bénéficie d'un effet juridique similaire à celui d'une signature manuscrite en termes* ***de présomption de fiabilité*** *sans qu'aucune preuve de la fiabilité de la signature ne soit rapportée. (Art 417-3 du DOC modifié par la loi n° 43-20) ;*
- *L'effet juridique d'une signature électronique qualifiée associée à un horodatage électronique qualifié est équivalent à celui d'une* ***signature manuscrite légalisée*** *(article 417-3 du DOC modifié par la loi n° 43-20) ;*
- *Le cachet électronique qualifié bénéficie d'une présomption d'intégrité des données et d'exactitude de l'origine des données auxquelles il est lié ;*

— *L'horodatage électronique qualifié bénéficie d'une présomption d'exactitude de la date et de l'heure qu'il indique et d'intégrité des données auxquelles se rapportent cette date et cette heure ;*

— *L'envoi recommandé électronique qualifié bénéficie d'une présomption relative à l'intégrité des données, à l'envoi de ces données par l'expéditeur identifié, à leur réception par le destinataire identifié et à l'exactitude de la date et de l'heure de l'envoi et de la réception indiquées.*

En vertu de la loi n° 43-20, les services de confiance qualifiés et les prestataires qui les offrent, sont soumis à des exigences plus strictes (usage des dispositifs certifiés, des audits de sécurité réguliers, respect strict des normes et standards, etc.) que celles applicables aux services non qualifiés, ce qui justifie les effets juridiques privilégiés qui leurs sont reconnus.

6. En quoi diffèrent les règles de preuve pour les services de confiance qualifiés et non qualifiés ?

Pour les services de confiance qualifiés, en cas de litige, c'est à la partie qui conteste leur validité d'apporter la preuve. Par exemple, c'est au destinataire d'un envoi recommandé électronique de prouver que l'envoi n'a pas été effectué. Cette présomption de fiabilité est similaire à celle qui s'applique dans le monde physique.

Dans le cas des services de confiance électroniques non qualifiés, en cas litige, c'est la partie qui en fait usage qui doit apporter les preuves de leur validité. Par exemple, l'expéditeur de l'envoi recommandé électronique doit lui-même prouver que l'envoi recommandé électronique a bel et bien été effectué. Il n'y a pas de présomption de fiabilité équivalente à celle qui s'applique au monde physique.

CHARGE DE LA PREUVE -CAS DE LA SIGNATURE ELCTRONIQUE-	
Signature électronique qualifiée	**Signature électronique non qualifiée**
La paternité d'une signature est présumée prouvée, à moins qu'une personne la conteste et apporte la preuve du contraire. — La partie qui conteste la validité de la signature électronique endosse la charge de la preuve. — On parle de renversement de la charge de la preuve.	Dans le cas où la paternité d'une signature est mise en cause, il convient à la personne qui soutient son authenticité de prouver la paternité de ladite signature. — Le signataire supporte la charge de la preuve de la validité de sa signature.

7. Comment choisir entre les services de confiance électroniques qualifiés et non qualifiés?

En règle générale, le choix est libre sauf obligation légale ou réglementaire dans certains secteurs exigeant le recours à un niveau donné. Lorsque le risque de litige est fort (risque d'actions collectives, transactions à forts montants), l'usage de la signature qualifiée serait de facto nécessaire. Les parties qui veulent réduire au maximum ce risque ont tout intérêt à faire appel à des services qualifiés. Le choix revient donc entièrement à l'utilisateur et fait partie d'un processus de gestion du risque métier qui peut prendre en considération les éléments ci-après :

	Niveau simple	**Niveau avancé**	**Niveau qualifié**
Cas d'utilisation lorsque	— L'enjeu financier et/ou juridique est faible — Le risque de contestation est faible	— L'enjeu financier et/ou juridique est important — Le risque de contestation est important	— L'enjeu financier et/ou juridique est critique — Le risque de contestation est à fort enjeu — Obligation réglementaire s'il y'a lieu

Prenant l'exemple de la signature électronique, en fait, tous les niveaux de signature électronique peuvent être utilisés pour signer électroniquement tous les types de documents, sauf certains actes devant répondre à un formalisme spécifique (actes notariés, marchés publics, etc.). L'estimation de la vraisemblance du litige (probabilité sur une période donnée) et de sa gravité (impacts liés à l'annulation de l'acte signé électroniquement) permet de préciser le choix du niveau approprié. Plus la vraisemblance et la gravité estimées d'un litige sont importantes, plus le choix d'un niveau de signature disposant d'une force probante élevée devient judicieux et recommandé.

En conséquence, il convient donc d'être vigilant quant au choix du niveau de signature électronique utilisé et d'évaluer, en amont, si ce niveau répond bien aux prérequis de la transaction ou du contrat à conclure en termes de valeur, du risque juridique, financier et opérationnel, sans perdre de vue également les considérations liées à la convivialité de l'usage, le coût et la sécurité.

En cas de recours à un service de confiance qui n'est pas qualifié, il serait important de vérifier que les garanties de fiabilité fournies par le prestataire (références à des normes, certifications, assistance et fourniture du dossier de preuve, etc.) permettent d'apporter la confiance dans l'utilisation des services proposés et d'aider à obtenir gain de cause en cas de contentieux.

8. Quelles sont les obligations des prestataires de services de confiance (PSCo) agréés et non agréés ?

Un prestataire de services de confiance agréé est un prestataire de services de confiance offrant au moins un service de confiance qualifié. La loi formule des exigences générales applicables à l'ensemble des prestataires de services de confiance agréés, ainsi que des exigences spécifiques pour chaque service de confiance qualifié.

Un prestataire de services de confiance agréé doit avoir fait l'objet d'une évaluation de conformité aux exigences de la loi n° 43-20 et de ses textes d'application et avoir obtenu son agrément, pour un ou plusieurs services de confiance qualifiés, auprès de l'autorité nationale avant de pouvoir commencer à le ou les fournir, tandis qu'un prestataire de services de confiance non agréé se contente d'une déclaration préalable auprès de ladite autorité.

Les prestataires de services de confiance sont responsables de leur négligence, incapacité ou insuffisance professionnelles tant vis-à-vis de leurs contractants que des tiers. Ils sont également tenus de conserver les données relatives à la fourniture des services de confiance, et de notifier à l'autorité nationale les incidents de sécurité.

9. En quoi consistent les services de validation et de conservation de la signature ou de cachet électronique ?

Avec l'usage grandissant de la signature électronique, de nombreux documents émanant des administrations et des entreprises sont susceptibles de constituer des éléments de preuve en cas de contentieux. Pour encadrer cet usage, et au-delà de la problématique de l'archivage de ces documents électroniques eux-mêmes, deux nouveaux services sont introduits par la loi n° 43-20 : l'un concerne la validation, l'autre la conservation des signatures ou cachets électroniques qualifiés :

- <u>La validation de signatures ou de cachets électroniques qualifiés</u>

Le service de validation des signatures ou cachets électroniques qualifiés permet aux parties utilisatrices de recevoir le résultat du processus de validation d'une signature ou cachet électronique qualifié d'une manière automatisée, fiable, et efficace. On aura donc la certitude au moyen de ce service fourni par un tiers de confiance, et au-delà de la durée de vie limitée (en général de 2 à 3 ans maximum) des certificats électroniques, que la signature ou le cachet électronique était bien valide au moment de son apposition.

- <u>La conservation des signatures ou des cachets électroniques qualifiés</u>

Le service de conservation des signatures ou cachets électroniques qualifiés permet d'étendre la fiabilité et la pérennité de celles-ci au-delà de leur période de validité technologique. En effet, avec le temps, la probabilité que les algorithmes utilisés dans les signatures ou cachets électroniques puissent être corrompus ou devenus obsolètes augmente. Le prestataire fournissant ce service doit conserver non seulement les signatures et cachets électronique qualifiés, mais aussi les éléments de preuve associés afin de pouvoir les fournir à la justice en cas de contentieux.

10. Dans quels cas l'envoi recommandé électronique peut-il être utilisé ?

L'envoi recommandé électronique peut être utilisé par toutes les catégories d'utilisateurs (personnes physiques, administrations, entreprises). Lorsqu'il est qualifié, l'envoi recommandé électronique se présente comme la version dématérialisée, de l'envoi à la réception, de la lettre recommandée papier avec un effet juridique similaire à celle-ci.

L'envoi recommandé électronique qualifié présente l'avantage d'apporter un acheminement instantané, une identification fiable de l'expéditeur et du destinataire, des preuves électroniques[3] associées aux envois (preuves de dépôt, de réception, de refus et de non-réclamation), ainsi qu'une conservation électronique probatoire des différents éléments relatifs à ces envois.

11. Quels services de confiance peuvent être fournis par un prestataire de services de confiance ?

Les prestataires de services de confiance peuvent choisir un ou plusieurs services de confiance parmi ceux énumérés dans la loi n°43-20.

Le fait d'offrir un service de confiance (qualifié ou non qualifié) ne leurs impose pas de fournir les autres services de confiance (qualifiés ou non).

Lorsqu'un prestataire demande un agrément pour la fourniture d'un ou plusieurs services de confiance, la décision d'agrément finale porte seulement sur le (ou les) services objet de la demande.

12. Quelles sont les garanties qu'offrent les prestataires de services de confiance agréés ?

Un prestataire de services de confiance agréé par l'autorité nationale :

- *Est soumis à des audits réguliers permettant de vérifier et de s'assurer de sa conformité aux exigences définies par la réglementation en vigueur ;*
- *Peut émettre des certificats électroniques ou proposer des services avec présomption de fiabilité ;*
- *Figure dans une liste publiée au Bulletin Officiel.*

Le statut de prestataire agréé apporte ainsi un degré de confiance supplémentaire auprès des utilisateurs, certes la responsabilité du choix d'un PSCo agréé ou pas incombe finalement au client en fonction de ses besoins.

13. Quel est le régime de contrôle applicable aux prestataires de services de confiance ?

Le régime de contrôle prévu par la loi n° 43-20 est du ressort de l'autorité nationale (DGSSI). Celle-ci a pour mission :

- *Le contrôle a priori dans le cadre de la demande d'un agrément en qualité de PSCo au titre de la loi n° 43-20 précitée pour la fourniture des services de confiance qualifiés,*

[3] Ces preuves peuvent être perçues comme l'équivalent dans le monde physique d'un avis de passage.

et a posteriori dans le cadre des audits périodiques auxquels sont soumis les PSCo agréés au cours de leur période d'agrément ;

— *La prise des mesures, a posteriori et à chaque fois jugée nécessaire, en ce qui concerne les prestataires de services de confiance non agréés établis sur le territoire national et ce, lorsque l'autorité nationale est informée que ces derniers ou les services qu'ils fournissent ne satisfont pas aux exigences de la loi n° 43-20 et de ses textes d'application.*

Les prestataires de services de confiance non agréés ne font pas l'objet d'un contrôle a priori.

14. Quelles sont les modalités de contrôle spécifiques aux prestataires de services de confiance agréés ?

En vue d'être agréés, les prestataires de services de confiance doivent se soumettre à une évaluation effectuée à leurs frais, par un organisme désigné par l'autorité nationale, au moins tous les 3 ans. Cette évaluation vise à s'assurer du respect de la loi n° 43-20 et des textes pris pour son application, et des règles de sécurité applicables aux services de confiance telles que fixées dans les référentiels d'exigences.

En dehors de ces audits réguliers (d'agrément ou de renouvellement d'agrément), l'autorité nationale peut décider à tout moment de soumettre le prestataire de services de confiance agréé à des contrôles spécifiques par rapport à un aspect donné, ou peut demander à des experts externes de procéder à une évaluation de la conformité dudit prestataire, aux frais de ce dernier.

III. QUESTIONS RELATIVES A LA SIGNATURE ET AU CACHET ELECTRONIQUE

15. Quels sont les différents niveaux de signature électronique ?

La loi n° 43-20 prévoit trois niveaux de signatures électroniques, ayant chacun des caractéristiques, effets juridiques, et usages différents :

— **La signature électronique simple** : Consiste en l'usage d'un procédé fiable d'identification garantissant le lien entre la signature et le document électronique auquel elle se rattache. Ce type de signature correspond au premier stade de sécurité et de reconnaissance légale de la signature d'un document. Elle ne requiert pas une décision de l'autorité nationale.

La signature électronique simple permet de justifier de l'intégrité[4] du document. Toutefois, l'identité du signataire est difficilement garantie, par conséquent la non-répudiation[5] ne peut être assurée dans tous les cas.

Comme son nom l'indique, la signature électronique simple est le procédé le plus facile à mettre en œuvre. Elle est adaptée aux actes simples **à faible enjeu juridique ou financier**.

— **La signature électronique avancée** : Est une signature simple qui doit respecter en outre les conditions suivantes :

- *être liée au signataire de manière univoque ;*
- *permettre d'identifier le signataire ;*
- *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 ;*
- *reposer sur un certificat électronique ou tout procédé jugé équivalent fixé par voie réglementaire ;*

[4] Que le document n'a pas été modifié depuis sa signature.

[5] Une fois que le document est signé, la personne l'ayant signé ne peut pas nier l'avoir signé.

- *être liée aux données qui lui sont associées de telle sorte que toute modification ultérieure des données soit détectable.*

A l'instar de la signature simple, la signature avancée ne requiert pas de décision de l'autorité nationale. La signature avancée est très adaptée au mode de signature électronique à distance et aux actes ou transactions comportant des **risques juridiques et/ou financiers importants.**

En cas de contestation, l'examen et l'appréciation du juge de la validité de ce type de signature et de son dossier de preuve correspondant (en principe conservé et produit par le PSCo pour la résolution de litiges) est nettement facilité dès lors que les conditions supplémentaires ci-dessus soient respectées.

— **La signature électronique qualifiée :** est une signature électronique avancée qui, en plus, doit reposer sur un certificat qualifié de signature électronique délivré par un PSCo agréé et mise en œuvre grâce à un dispositif qualifié de création de signature électronique. Un tel dispositif garantit, avec un haut niveau de confiance, que la signature ne peut être réalisée que par le signataire légitime. Ce dispositif doit être attesté par un certificat de conformité délivré par l'autorité nationale.

Etant présumée fiable jusqu'à preuve du contraire, la signature électronique qualifiée représente ainsi le plus haut niveau de reconnaissance juridique et de sécurité de la signature électronique, permettant à la fois de s'assurer de façon fiable de l'identité du signataire grâce au certificat qualifié de signature électronique et de garantir la sécurité des données contenues dans le document signé via l'utilisation d'un dispositif qualifié de création de signature électronique. L'acte signé est suffisant pour démontrer le consentement des parties à son contenu.

Utiliser la signature électronique qualifiée revient donc à s'offrir un niveau de protection juridique élevé en cas de contentieux. Par conséquent, ce type de signature devrait être réservé aux actes et transactions électroniques **à très fort enjeu juridique ou/et financier**.

16. Quelle distinction y'a-t-il entre la signature électronique et le cachet électronique ?

S'il est vrai que la technologie ainsi que les outils matériels et logiciels utilisés pour créer un cachet électronique sont identiques à ceux utilisés pour la création d'une signature électronique, le cachet électronique se distingue fondamentalement de la signature électronique par le fait que cette dernière est réservée aux personnes physiques, par contre, le cachet électronique est dédié aux personnes morales. En effet, la signature électronique permet, tout comme la signature manuscrite, d'attester du consentement d'une personne physique (signataire), tandis que le cachet électronique, assimilable au tampon traditionnel d'administration ou d'entreprise, est utilisable par les personnes morales tel un tampon électronique permettant d'attester de l'intégrité et l'origine des données.

17. Qui peut demander un certificat électronique qualifié ?

La loi n° 43-20 n'impose aucune restriction quant aux demandeurs de certificats électroniques, dès lors qu'ils sont identifiés conformément aux exigences de l'article 33 de cette loi, et respectent les conditions générales d'utilisation liées à ces certificats. Ainsi, toute personne physique ou morale peut demander un certificat qualifié de signature électronique ou de cachet électronique, délivré par un prestataire de services de confiance agréé.

Le certificat électronique permet dans le cas de la signature électronique de signer des documents numériques en ayant la garantie que l'identité du signataire est reconnue sans ambiguïté ni contestation.

Pour rappel, un certificat qualifié de signature électronique est une attestation de l'identité du signataire délivrée par un processus répondant à des exigences garantissant la validité de la signature,

l'identité de son signataire, a minima son nom, son pseudonyme ou l'un de ses identifiants administratifs (ICE, numéro de registre de commerce…) dans le cas d'une entreprise par exemple.

18. Un face à face est-il nécessaire pour la délivrance d'un certificat électronique qualifié ?

Pour la délivrance d'un certificat électronique qualifié pour un service de confiance, l'identité et tous les attributs de la personne physique ou morale à laquelle ledit certificat est délivré doivent être vérifiés. La loi n° 43-20 précise que cette vérification doit se faire :

- *en présentiel (de la personne physique ou du représentant autorisé de la personne morale) ;*
- *à distance, à l'aide de moyens d'identification électronique dont la délivrance a nécessité la présence physique de la personne physique ou du représentant autorisé de la personne morale devant l'entité ayant délivré ce moyen. A ce titre, cette vérification d'identité à distance doit permettre de vérifier que le moyen présenté par l'intéressé est authentique et que ce dernier en est le détenteur légitime. Ces moyens sont fixés par voie réglementaire (exemple CNIE 2 ou toute pièce d'identité officielle permettant la vérification de l'identité à distance) ;*
- *Au moyen d'un certificat qualifié de signature électronique ou de cachet électronique en cours de validité, délivré conformément aux deux points ci-dessus ;*
- *A l'aide d'autres méthodes d'identification qui fournissent une garantie jugée équivalente par l'autorité nationale aux moyens précités en termes de fiabilité quant à la présence physique.*

Ainsi, un face à face peut être remplacé par une vérification d'identité à distance, ce qui ouvre la voie à des services entièrement dématérialisés.

19. Une signature manuscrite numérisée ou scannée a-t-elle une valeur juridique ?

Non. Cette signature ne présente **aucune garantie** en termes d'identité du signataire et elle ne permet pas non plus de manifester **le consentement** de ce dernier aux obligations qui découlent de l'acte signé.

Les conditions requises par l'article 417-2 du DOC ne sont donc pas respectées. Cela découle notamment du fait qu'une telle signature peut facilement être falsifiée (via un logiciel de retouche d'image) ce qui rend très facile l'usurpation d'identité.

En tout état de cause, une signature électronique n'a pas d'apparence physique.

20. En quoi consiste la signature électronique à distance ou dans le Cloud ?

Un service de signature électronique à distance ou dans le Cloud est assuré via un système dans lequel l'environnement de création de signatures électroniques est géré par un prestataire de services de confiance au nom du signataire, et grâce auquel le signataire peut activer à distance la réalisation de sa signature électronique. Dans ce mode de signature, la clé privée qui sert à créer la signature électronique est gérée et hébergée dans le Cloud par un prestataire de service de confiance et non directement sur un support physique détenu par le signataire, dit dispositif de création de signature électronique (tokens, cartes à puce,…). Ainsi, le signataire peut signer un document depuis n'importe quel appareil (PC, tablette ou Smartphones), n'importe où, et sans aucun prérequis technique.

21. En quoi consiste la signature électronique qualifiée à distance ?

Le Cloud sous certaines conditions peut être aussi sécurisé qu'un support physique de signatures telles que les cartes à puce. Par ailleurs, la loi n° 43-20 ne positionne plus ces supports comme seules solutions nécessaires pour effectuer une signature qualifiée. La signature électronique qualifiée peut

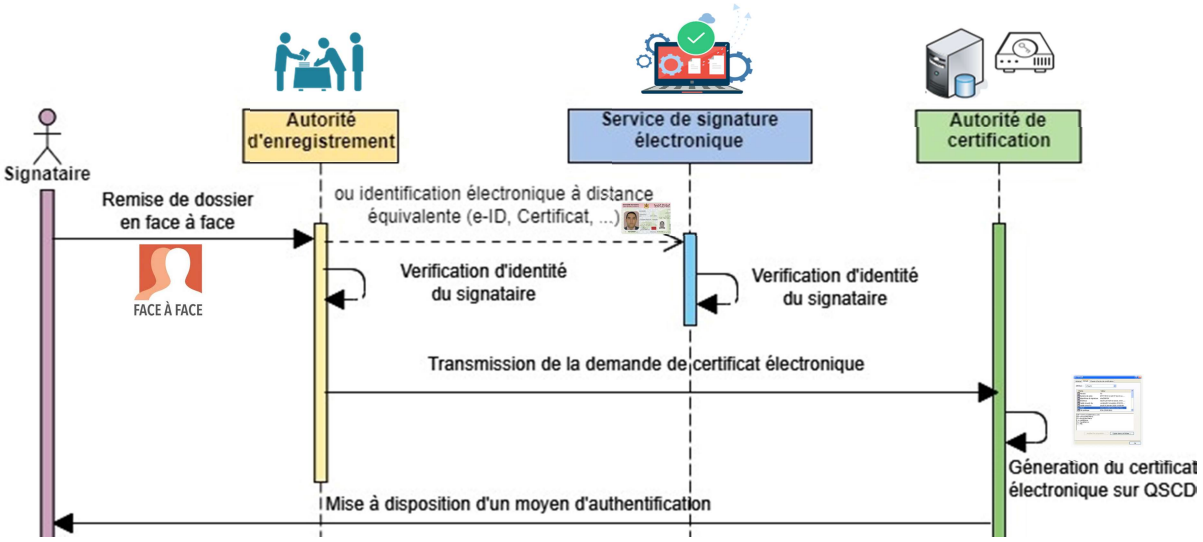
être désormais, sous certaines conditions, gérée à distance par un prestataire de service de confiance agréé pour le compte du signataire (voir figures ci-dessous).

En effet, la loi permet explicitement (aliéna 3 de l'article 8) la réalisation de signatures qualifiées « à distance » pour le compte du signataire. Les clés privées de signatures ou les données de création de signature électronique en jargon juridique étant gérées par un prestataire de services de confiance agréé, et ce, en garantissant que l'utilisation de ces données soit sous contrôle exclusif du signataire légitime, et que les exigences en matière de signature électronique qualifiée soient satisfaites.

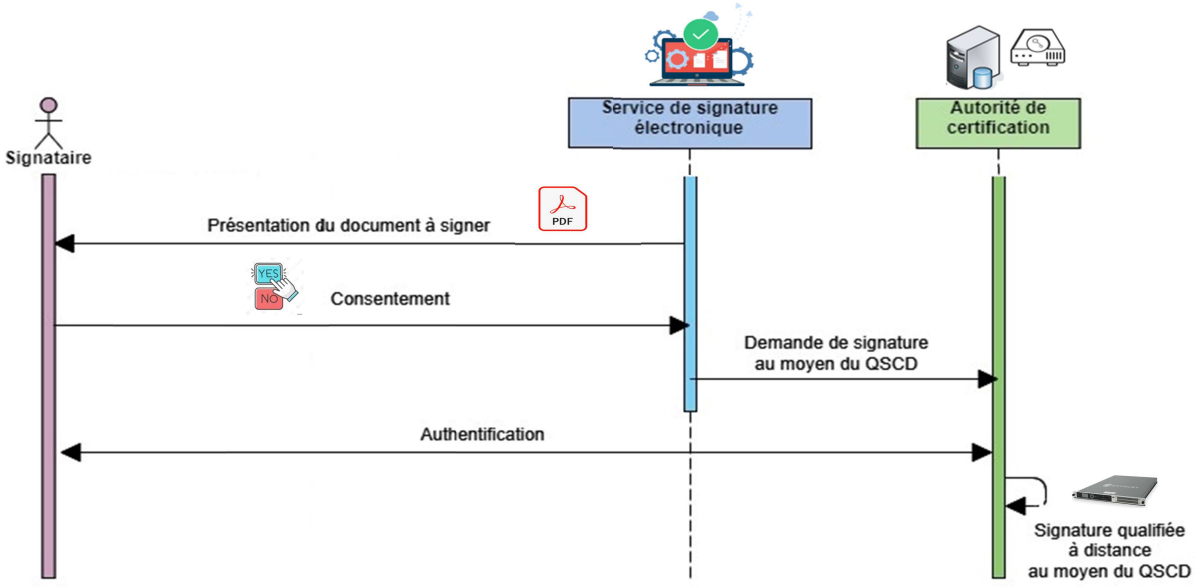
La vérification du respect de ces exigences est réalisée dans le cadre de la certification de conformité du dispositif de création de signature électronique (QSCD[6]) déployé.

Les figures ci-dessous décrivent globalement la procédure d'enregistrement des clients lors de la demande de souscription au service de confiance ainsi que le fonctionnement de la signature électronique qualifiée à distance :

- Enregistrement du client :



- Opération de signature électronique :



[6] Qualified signature creation device.

22. Comment attester du consentement du signataire lors d'une signature électronique avancée à distance ?

A l'image d'une signature en mode local, où la réalisation de la signature électronique est réalisée sous le contrôle exclusif du signataire (reposant par exemple sur une carte à puce et un code PIN), la création d'une signature électronique avancée à distance, doit fournir un niveau de sécurité similaire à celui d'une signature locale.

Pour ce faire, plusieurs solutions techniques peuvent être envisagées (par exemple, la saisie d'un code PIN réservé à cet usage dans une application dédiée, confirmation par SMS OTP…), dans la mesure où l'implémentation faite de ces solutions est sécurisée.

23. Quels sont les critères à considérer pour choisir un niveau de signature électronique?

Le tableau récapitulatif ci-dessous reprend les principales caractéristiques des différents niveaux de signature électronique :

Niveau de signature	Signature simple	Signature avancée	Signature qualifiée
Infrastructure	Pas d'exigence	Infrastructure centrale répondant à un cahier des charges technique	Infrastructure centrale qualifiée très cadrée
Niveau de certificat	Neutralité technologique	Certificat électronique ou équivalent (à la volée ou sur support logiciel ou matériel : poste de travail, mobile, …)	Certificat qualifié sur support matériel (Carte à puce, USB crypto ou hébergé chez un PSCo agrée en mode à distance)
Vérification de l'identité	Pas d'exigence	Identité vérifiée rigoureusement (à distance)	Identité vérifiée en face à face ou niveau jugé équivalent
Exigence dispositif de signature	Pas d'exigence	Contrôle exclusif du signataire de sa clé privée doit être garanti	Dispositif de signature attesté par un certificat de conformité délivré par l'autorité nationale
Bénéfices	- Facile à mettre en œuvre - Expérience utilisateur - Adapté aux actes simples à faible risque juridique ou financier.	- Bonnes garanties en cas de litige - Dossier de preuve solide à la charge du PSCo - Garantit l'intégrité des actes et la non-répudiation - Expérience utilisateur - Adapté aux actes ou transactions à moyen ou important enjeu juridique, financier…	- Présomption de fiabilité : effet juridique équivalent à la signature manuscrite - La charge de la preuve pèse sur celui qui la conteste - Destinée aux actes et transactions à très fort enjeu juridique, financier, etc.
Limites & contraintes	- Preuve à la charge du porteur ou fournisseur du service (celui qui prétend que sa signature est valide) - La non-répudiation non garantie	- Preuve à la charge du fournisseur du service - La charge de la preuve revient à celui qui prétend que sa signature est valide	- Complexe à mettre en œuvre - Nombreux audits à prévoir/conformité stricte aux normes de sécurité internationales (ETSI, CC, ISO, FIBS…)

24. Quelques exemples de cas d'usage potentiels des services de confiance ?

Les usages possibles des services de confiance sont divers, et ils concernent tous les secteurs. À titre indicatif, les services de confiance peuvent être utilisés dans les domaines suivants[7] :

Services de Confiance	Exemples de cas d'usage
Signature électronique	- Attestations, Avis, notifications administratives - Transfert de dossiers juridiques - Procès-verbaux - Casiers judiciaires - Actes d'état civil - Déclarations - Actes notariés - Contrats commerciaux - Vote électronique - Soumission électronique aux marchés publics - Contrats de crédit, assurance, travail, bail …
Cachet électronique	- Factures électroniques - Devis, Notes d'honoraire - Relevés de comptes bancaires - Diplômes - Pass sanitaire - Textes juridiques
Horodatage électronique	- Dater une signature électronique - Factures électroniques, - Bulletins de paie numériques, - Copies conformes de documents numériques à valeur juridique - Clôture des enchères électroniques
Envoi recommandé électronique	- Envoi d'une promesse d'embauche ou du contrat de travail - Conclusion ou résiliation des contrats d'assurance - Gestion des comptes bancaires (opération de clôture…) - Envoi de divers actes juridiques et administratifs - Marchés publics : Notifications de différents documents, par exemple : décision d'attribution ou de rejet, notification du marché, reconduction de marché, avenant, mise en demeure, résiliation de marché…

25. Qu'est-ce qu'un dispositif de création de signature électronique ?

Un dispositif de création de signature électronique est un dispositif logiciel ou matériel servant à créer une signature électronique tout en garantissant l'intégrité et la confidentialité des données de création de signature électronique (la clé privée), ainsi que la sécurité de la signature.

Un dispositif qualifié de création de signature électronique (QSCD) doit satisfaire aux exigences de l'article 8 de la loi n° 43-20, il est exigé pour créer la signature électronique qualifiée. La conformité du QSCD à ces exigences règlementaires, techniques et de sécurité est certifiée par l'autorité nationale via la délivrance d'un certificat de conformité.

En pratique, il s'agit souvent d'une carte à puce ou d'une clé cryptographique hautement certifiée, et plus récemment, d'équipements cryptographiques (HSM) installés dans l'environnement du prestataire agréé, faisant partie ainsi d'un système global formant le dispositif qualifié de création de signature (QSCD) doté d'une gestion d'accès hautement sécurisée afin de permettre au signataire de préserver le contrôle exclusif de ses données de création de signature électronique pour ses besoins de signature et ce ,via des mécanismes d'authentification forts.

Le certificat de conformité est délivré pour une version identifiée du QSCD, et sa durée de validité ne peut excéder cinq (5) ans au-delà de la décision de certification ou de la dernière surveillance selon les normes exigées, à savoir les critères communs.

Pour les dispositifs qualifiés de création de signature électronique gérés par un PSCo agréé pour le compte d'un signataire (dans le cas d'une « signature à distance ou dans le Cloud »), l'autorité nationale définit le processus de certification de la conformité pour ce type de dispositif.

[7] Cette liste, donnée à titre indicatif, n'est pas exhaustive.

La fiabilité de l'environnement de signature électronique doit également être prise en compte. Un environnement sécurisé permet, par exemple, de garantir que l'utilisateur signe bien ce qu'il voit sur son écran, et non un autre document. Il est donc important au moment de la signature électronique de se questionner sur l'environnement.

26. Quels sont les régimes applicables à la cryptologie dans la loi n° 43-20 ?

Les opérations d'importation, d'exportation ou de fourniture de moyens de cryptologie, ainsi que de fourniture de prestations de cryptologie sont soumises dans le cadre de la loi n° 43-20 à un régime de déclaration préalable ou de demande d'autorisation. Ces démarches sont à accomplir auprès de l'autorité nationale.

Le régime applicable dépend des fonctionnalités techniques du moyen et de l'opération commerciale projetée, selon les cas suivants :

— ***Déclaration préalable*** *: Moyen ou prestation de cryptologie dont l'unique objectif est d'authentifier une transmission ou d'assurer l'intégrité des données transmises par voie électronique (authentification et intégrité).*

— ***Autorisation*** *: Autre objet que celui visé ci-dessus (confidentialité et cryptanalyse).*

Les démarches à effectuer auprès de l'autorité nationale (DGSSI) incombent au fournisseur du moyen ou prestation de cryptologie. Ces démarches peuvent également être accomplies par l'importateur ou l'exportateur du moyen de cryptologie, à condition qu'il soit en mesure de fournir les informations techniques relatives à ce moyen.

Certains moyens et prestations de cryptologie sont dispensés de toute formalité précitée. La liste de ces moyens et prestations est fixée par voie réglementaire (voir l'annexe 6 du décret n° 2.22.687).