

SIGNATURE A DISTANCE

ETAT DES LIEUX ET BONNES PRATIQUES

Version	Date	Description	Auteurs	Sociétés
1.0	30/10/2019	Pour diffusion	ClubPSCo / AFAI-ISACA	SEALWeb

État du document	Classification
Pour discussion	CONFIDENTIEL

Ce document est la propriété exclusive du ClubPSCo et de l'AFAI-ISACA



Son usage est réservé à l'ensemble des personnes habilitées selon leur niveau de confidentialité.

Sa reproduction est régie par le Code de la propriété intellectuelle qui ne l'autorise qu'à l'usage privé du copiste.

Sommaire

1	PREAMBULE	4
2	EXEMPLES D’USAGES METIERS	5
2.1	CONTRACTUALISATION BANCAIRE ELECTRONIQUE A DISTANCE	5
2.2	PROCES-VERBAL PRODUIT EN MOBILITE PAR UN AGENT ASSERMENTE	7
2.3	EXECUTION D’ORDRES DANS LE CADRE D’UN CONTRAT	8
2.4	FACTURES	9
2.5	CONTRATS DE TRAVAIL	11
2.6	FEUILLE DE PRESENCE A UNE FORMATION PROFESSIONNELLE.....	14
2.7	RECEPTION DE LETTRES RECOMMANDES ELECTRONIQUES (LRE) QUALIFIEE	15
2.8	ATTESTATIONS A DISTANCE	16
3	CONDITIONS DE MISE EN ŒUVRE DE LA SIGNATURE A DISTANCE EN FONCTION DES NIVEAUX DE SIGNATURE	19
3.1	SIGNATURE SIMPLE	19
3.2	SIGNATURE AVANCEE	19
3.3	SIGNATURE QUALIFIEE.....	20
3.4	NORMES ET STANDARDS APPLICABLES	20
3.4.1	<i>La délivrance d’un certificat</i>	21
3.4.2	<i>La protection des clés privées</i>	22
3.4.3	<i>Formats et standards de la signature</i>	22
3.4.4	<i>La création de signature</i>	23
3.4.5	<i>L’audit des prestataires</i>	24
4	BONNES PRATIQUES DE MISE EN ŒUVRE DE LA SIGNATURE A DISTANCE	25
4.1	BONNES PRATIQUES ORGANISATIONNELLES	25
4.1.1	<i>L’identification du signataire</i>	25
4.1.2	<i>L’authentification du signataire à la création de la signature</i>	25
4.1.3	<i>Recueil du consentement</i>	26
4.1.4	<i>Compréhension du parcours par le signataire</i>	27
4.2	BONNES PRATIQUES TECHNIQUES	27
4.2.1	<i>Visualisation des informations signées</i>	27
4.2.2	<i>Création de la signature électronique</i>	28
4.2.3	<i>La maîtrise de l’environnement logiciel et matériel</i>	29
4.2.4	<i>Gestion des preuves (création, conservation, restitution, contenu des preuves)</i>	30
4.2.5	<i>Conformité au règlement sur la protection des données à caractère personnel (RGPD)</i>	31

5	DIFFERENTS SCENARIOS DE SIGNATURE A DISTANCE	32
5.1	SIGNATURE SIMPLE AVEC MECANISME D’INTEGRITE	32
5.1.1	<i>Principes</i>	32
5.1.2	<i>Avantages & inconvénients</i>	33
5.2	SIGNATURE SUR LA BASE D’UN CERTIFICAT GENERE A LA VOLEE	34
5.2.1	<i>Préambule : le certificat généré à la volée</i>	34
5.2.2	<i>Principes</i>	34
5.2.3	<i>Avantages et inconvénients</i>	36
5.3	SIGNATURE AVANCEE AVEC VERIFICATION D’IDENTITE	36
5.3.1	<i>Principes</i>	36
5.3.2	<i>Avantages et inconvénients</i>	37
5.4	SIGNATURE AVANCEE AVEC VERIFICATION EN FACE A FACE PHYSIQUE	37
5.4.1	<i>Principes</i>	37
5.4.2	<i>Avantages et inconvénients</i>	38
5.5	SIGNATURE AVANCEE AVEC VERIFICATION EN FACE A FACE A DISTANCE	39
5.5.1	<i>Principes</i>	39
5.5.2	<i>Avantages et inconvénients</i>	40
5.6	SIGNATURE QUALIFIEE A DISTANCE	40
5.6.1	<i>Principes</i>	40
5.6.2	<i>Avantages et inconvénients</i>	41
5.7	SIGNATURE ELECTRONIQUE A PARTIR D’EID NOTIFIEES	41
5.7.1	<i>Principes</i>	41
5.7.2	<i>Avantages et inconvénients</i>	42
5.8	SIGNATURE ELECTRONIQUE A DISTANCE EN ENVIRONNEMENT MOBILE	42
5.8.1	<i>Principes</i>	42
5.8.2	<i>Avantages et inconvénients</i>	44
6	ANNEXES	45
6.1	TEXTES REGLEMENTAIRES	45
6.2	NORMES ET STANDARDS APPLICABLES	46
6.3	GLOSSAIRE	47

	<p>Signature à distance : état des lieux et bonnes pratiques</p>	
-----------------------------------------------------------------------------------	------------------------------------------------------------------	-------------------------------------------------------------------------------------

1 PREAMBULE

Ce document, rédigé par l'association ClubPSCo et publié avec l'AFAI-ISACA, a été produit dans un objectif pédagogique, pour permettre une compréhension partagée des moyens envisageables pour mettre en œuvre spécifiquement des procédés de « signature à distance ».

Il n'entend pas être exhaustif des moyens possibles, mais propose, sous la forme d'exemples le plus souvent, les bonnes pratiques recommandées par ses membres pour faciliter le déploiement de ce type de solutions à grande échelle.

- Qu'entend-on par « signature à distance » ?

La « signature à distance » se met en opposition à la « signature cliente » ou « signature locale ».

Dans le cadre d'une « signature à distance », la bi-clé et le certificat associé au signataire sont générés, stockés et mis en œuvre sur une infrastructure distante, côté serveur.

Le signataire ne dispose donc pas directement des moyens de signature.



Règlementairement, la « signature à distance » prétend aux mêmes conditions que la « signature locale », c'est-à-dire que l'on retrouve dans ce contexte les mêmes niveaux de signatures : simple, avancée, qualifiée.

- Problématiques soulevées (identification / authentification / contrôle exclusif / interopérabilité / usages pour des téléservices « tiers »...)

Si l'on peut prétendre aux mêmes niveaux de signature dans le contexte de la « signature à distance », c'est qu'il est nécessaire de couvrir les mêmes exigences techniques, sécuritaires et réglementaires. Les exigences explicitées par le règlement eIDAS et les normes ETSI sont alors à couvrir ici, notamment sur les aspects suivants :

- Identification du signataire, et moyens associés permettant de garantir l'identité du signataire pour l'établissement du certificat de signature ;
- Conditions et niveaux d'authentification du signataire pour obtenir son consentement à signer, et par là même son consentement à utiliser sa bi-clé de signature stockée côté serveur ;
- Les garanties de contrôles exclusifs pour répondre aux exigences des niveaux avancés et qualifiés au sens eIDAS ;
- L'interopérabilité des systèmes de signature mis en œuvre entre les différents pays ;
- Périmètre : Européen.

En se basant sur les attendus du règlement eIDAS, le présent document vise à établir les bonnes pratiques à respecter dans le cadre de la signature à distance au niveau européen. Néanmoins ces mêmes exigences sont souvent attendues dans des contextes plus larges. Par exemple le référencement des processus de signature et de validation de signature dans des outils tiers nécessitent souvent de respecter les mêmes niveaux d'exigences.

	<p>Signature à distance : état des lieux et bonnes pratiques</p>	
-----------------------------------------------------------------------------------	------------------------------------------------------------------	-------------------------------------------------------------------------------------

2 EXEMPLES D'USAGES METIERS

2.1 Contractualisation bancaire électronique à distance

Objet du cas d'usage : fournir un service permettant de souscrire à un produit de financement à distance.

Secteur d'activité : les particuliers sont principalement ciblés par ce cas d'usage, notamment avec l'émergence des banques en ligne, permettant des ouvertures de comptes bancaires à distance mais également pour la souscription à d'autres produits de financement (*ex : crédit à la consommation, ...*). Certains secteurs d'activité s'appuient davantage sur la contractualisation à distance comme le secteur de l'automobile, secteur dans lequel des financements sont proposés pour l'acquisition ou la location de véhicules. Plus généralement, la contractualisation présentée ci-dessus peut s'appliquer aussi pour des contrats d'assurance, d'abonnements téléphoniques, etc.

Populations visées : les particuliers et les entreprises sont tout autant ciblés par ce cas d'usage qui n'impose aucun équipement particulier pour le signataire au préalable pour une contractualisation à distance.

Niveau(x) juridique atteint(s) : en pratique et selon le niveau du risque identifié par l'organisme financier, la signature simple ou la signature avancée sont mises en œuvre.

Néanmoins, les Organismes de contrôle nationaux et en particulier l'ACPR (*Autorité de Contrôle Prudentiel et de Résolution*) précisent qu'une entrée en relation d'affaires à distance doit se reposer sur une signature avancée basée sur un certificat qualifié.

Par ailleurs, l'ACPR précise qu'un organisme financier n'est pas dans l'obligation de mettre en œuvre ces mesures complémentaires de vigilance dans le cas où la relation d'affaires établie à distance présente un risque faible en matière de *blanchiment de capitaux et de financement du terrorisme*.

Intérêt de la contractualisation bancaire à distance : permettre à tout client/prospect de souscrire à un produit financier à n'importe quel moment sans se rendre en agence ou en point de vente.

Pour l'organisme financier, réduire les fraudes de falsification de contenu mais aussi réduire sa gestion du papier et disposer d'un contrat complet et signé à l'issue de la signature du client/prospect.

Volumétrie existante / cible : pour certains organismes financiers, la contractualisation électronique à distance s'inscrit dans un projet de transformation et impose un changement par palier. Dans ce cas, le client/prospect dispose du choix de contractualiser en papier selon la méthode existante ou par voie électronique via une contractualisation à distance.

En moyenne, ces organismes financiers voient 50% de leurs contrats passés la première année par une contractualisation à distance. Le reste demeure via un process papier. Ces chiffres sont donnés à titre indicatif, la réalité opérationnelle dépendant essentiellement de la stratégie de déploiement, propre à chaque organisme financier.

Certains organismes financiers plus récents (FinTech) proposent directement une contractualisation exclusivement à distance. C'est par exemple le cas des banques en ligne.

Gains réalisés : la contractualisation bancaire à distance doit reposer sur le principe de « *gagnant-gagnant* » pour une adhésion assurée des clients et prospects.

Pour un organisme financier, la contractualisation à distance permet :

- d'augmenter le taux de transformation des prospects ;
- de réduire les coûts de gestion du papier volumineux ;
- d'automatiser les contrôles et ainsi de gagner en efficacité sur la qualité et la durée des traitements effectués ;
- de réduire l'intervention des opérateurs Back Office pour les contrôles des dossiers ;
- de pouvoir systématiquement collecter/récupérer le contrat signé.

Pour un client/prospect, la contractualisation à distance permet :

- d'éviter un déplacement en agence ;
- de souscrire à un produit de financement 24h/24 7j/7 ;
- de gagner du temps : plus besoin d'attendre un rendez-vous ;
- d'avoir un délai de traitement réduit : automatisation des contrôles.

Cinématique typique : le client/prospect souscrit à un produit financier et fournit dans ce contexte ses informations ainsi que ses pièces justificatives (*en particulier un document d'identité*). Ces informations sont soumises à des contrôles automatiques et manuels avant l'accord de l'organisme financier préalable à la contractualisation avec le client/prospect. Le contrat est généré et un scellement au nom de l'organisme financier est apposé afin de garantir l'origine du contrat et d'en assurer l'intégrité. Le contrat est ensuite transmis au client/prospect pour signature. Ce dernier est notifié du document à signer et se rend sur le service de signature via l'URL reçue dans son email de notification. Le client est authentifié par un OTP SMS qui déclenche la génération d'un certificat et la signature électronique du contrat.

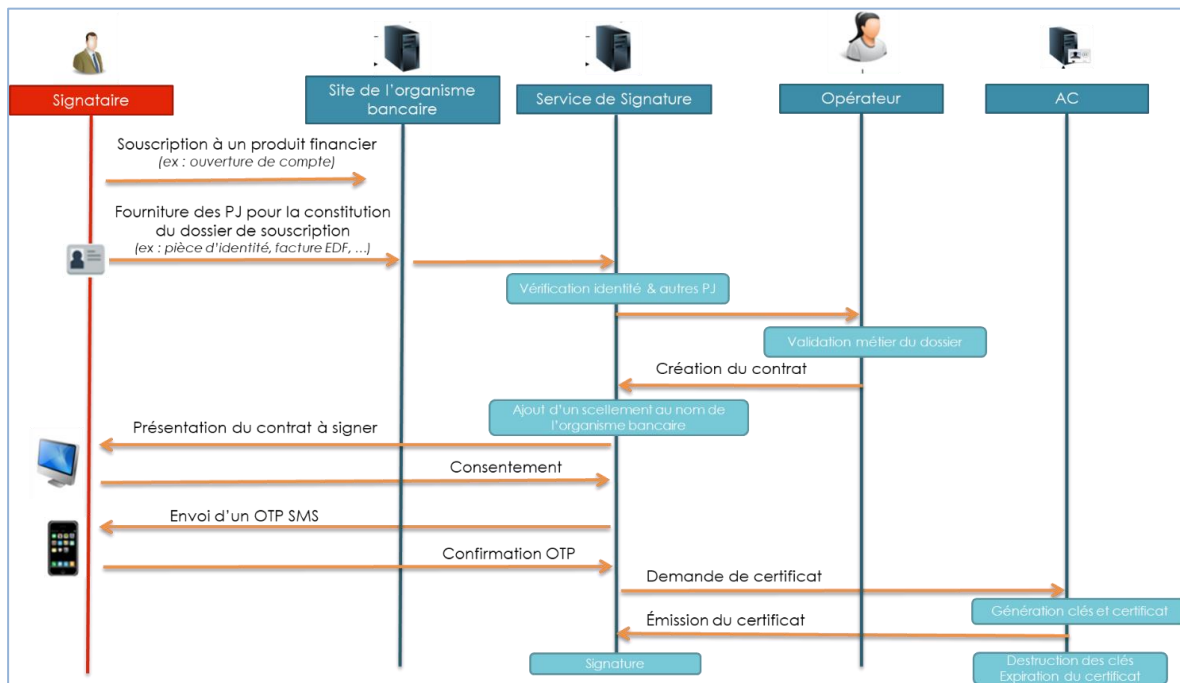




Figure 1 : Contractualisation bancaire électronique à distance

Problématiques spécifiques relatives au déploiement : l'organisme financier a besoin d'identifier le client/prospect. Cette identification doit reposer *a minima* sur la collecte d'un justificatif d'identité (CNI, passeport, titre de séjour).

	<p>Signature à distance : état des lieux et bonnes pratiques</p>	
-----------------------------------------------------------------------------------	----------------------------------------------------------------------	-------------------------------------------------------------------------------------

L'efficacité d'un service de contractualisation bancaire électronique à distance s'appuie en grande partie sur la capacité de l'organisme financier à contrôler les pièces justificatives envoyées par les clients/prospects.

Bien qu'implicite, le service d'horodatage est indispensable à un tel service de façon à prouver la date et l'heure de la transaction.

Types de certificats mis en œuvre : *a minima* des certificats « certifiés » selon la norme ETSI EN 319 411-1 niveau LCP, voire des certificats de niveau NCP sous réserve de réalisation d'un face à face avec le porteur.

Contraintes techniques spécifiques au cas d'usage : pour les cas d'usage les plus sensibles, il est recommandé d'émettre des certificats aux clients/prospects par une Autorité de Certification (AC) reconnue par Adobe (*référencement AATL - Adobe Authorized Trust List*), ce qui nécessite le respect des exigences AATL v2 imposant un face à face avec le porteur.

Les contrats, généralement au format PDF, sont consultés *a posteriori* par les clients/prospects via le lecteur d'Adobe (*Adobe Reader*). Ce dernier affichera au client/prospect un message lui précisant que « la signature a un problème » si celle-ci a été réalisée via un certificat émis par une AC non-reconnue par Adobe.

Bien que la qualité de la signature ne soit pas impactée, la confiance du client le serait et son adhésion à la démarche de signature électronique à distance pourrait être remise en question pour ce facteur « psychologique ».

2.2 Procès-verbal produit en mobilité par un agent assermenté

Objet du cas d'usage : établir un procès-verbal de constat d'infraction par un agent assermenté, équivalent au procès-verbal papier. La signature apposée ne doit pas être contestable par le contrevenant.

Secteur d'activité : Police, gendarmerie. Ce type de scénario peut aussi être étendu pour des agents assermentés tels que des huissiers ou des contrôleurs de l'administration fiscale.

Populations visées : agents assermentés et citoyens français ou étrangers



Niveau(x) juridique atteint(s) : Signature qualifiée eIDAS ou RGS**

Prérequis juridique : l'agent doit être assermenté pour faire valoir sa fonction.

Intérêt de l'usage à distance du service de confiance : le constat d'infraction et l'établissement d'un procès-verbal associé se font généralement en mobilité (hors radars automatiques). L'environnement de mise en œuvre nécessite à l'agent d'être le plus libre possible d'équipements pour pouvoir assurer sa mission de contrôle physique des infractions. Les matériels permettent de capturer les informations à même d'établir l'infraction très rapidement (prise en photo de la plaque d'immatriculation). Cela suffit ensuite à l'agent assermenté pour établir le procès-verbal. Ce système de verbalisation existe depuis plus de 5 ans et vise à remplacer le procès-verbal manuscrit (timbre amende).

Volumétrie existante / cible : le volume est important du fait du déploiement à l'échelle nationale en police et gendarmerie.

Gains réalisés : les gains sont essentiellement pour l'ordre public qui automatise le constat et la mise en paiement de l'infraction. N'ayant pas de nécessité d'être physiquement avec le contrevenant, cela permet d'éviter les cas de litiges en présence de l'agent assermenté.

	<p>Signature à distance : état des lieux et bonnes pratiques</p>	
-----------------------------------------------------------------------------------	------------------------------------------------------------------	-------------------------------------------------------------------------------------

En synthèse les avantages notables sont :

- Un système fiable, mais également rigoureux pour toutes les personnes verbalisées, en raison de l'automatisation du traitement des amendes et de leur archivage dématérialisé et sécurisé ;
- Plus de risque de perte ou de vol du procès-verbal papier sur le pare-brise et donc moins de risque d'amendes majorées ;
- L'enregistrement électronique des données évite des erreurs de transcription ;
- Un net allègement des tâches administratives de suivi.

Cinématique typique : le procès-verbal électronique, est un procès-verbal réalisé sous forme numérique et traité par le Centre national de traitement de Rennes ; il donne lieu à l'expédition d'un avis de contravention au domicile du contrevenant. Il remplit les processus suivants :

- L'enregistrement du procès-verbal ;
- La notification de la contravention ;
- Le recouvrement des amendes.

Les matériels permettant cette verbalisation électronique sont :

- Des appareils numériques portables (PDA ou "Personal Digital Assistant") ;
- Des micro-ordinateurs portables (PC-tablettes) ;
- Des terminaux informatiques embarqués (TIE) ;
- Des interfaces de saisie sur poste de travail informatique fixe (IHM-Web).

Types de certificats mis en œuvre : certificats qualifiés RGS** ou RGS***, ou certificats qualifiés de signature eIDAS selon la norme ETSI EN 319 411-2 au niveau QCP-n-qscd.



2.3 Exécution d'ordres dans le cadre d'un contrat

Objet du cas d'usage : passer des ordres (par exemple boursiers dans le secteur bancaire) dans le cadre d'un contrat existant (B2B, B2C, quel que soit le domaine d'activité).

Le cas d'usage considéré concerne les contrats où un risque important existe, non pas seulement à la souscription, mais également sur chacun des ordres passés. Ces risques sont typiquement liés aux montants financiers mis en jeu par un ordre, ou à son effet juridique (ou financier) en lien avec sa date exacte d'exécution. Il est alors nécessaire pour les organisations contractantes de se protéger afin :

- D'assurer la non-répudiation de l'ordre passé : se mettre en capacité de prouver aisément que le donneur d'ordre a effectivement lui-même donné l'ordre d'exécution ;
- D'assurer l'intégrité de l'ordre donné, afin que ni le montant ni les caractéristiques de l'ordre (achat ou vente, nombre de titres, identifiant du titre, limite d'achat, durée de l'offre) ne puissent être remis en question ;
- D'assurer de façon fiable la date passage de l'ordre.

Secteur d'activité : Le secteur adressé couvre aujourd'hui le domaine financier (banque, assurance), mais on peut facilement imaginer qu'un mécanisme similaire soit adapté à d'autres domaines, par exemple pour le passage de bons de commande réalisés sous couvert d'un contrat-cadre entre une société et ses sous-traitants.

	<p>Signature à distance : état des lieux et bonnes pratiques</p>	
-----------------------------------------------------------------------------------	------------------------------------------------------------------	-------------------------------------------------------------------------------------

Populations visées : les particuliers et les entreprises titulaires des contrats dans le cadre duquel sont passés les ordres.

Niveau(x) juridique atteint(s) : Aujourd’hui, il est courant que les ordres soient transmis sur la base d’une simple authentification sur le site. Les solutions de signature électronique à distance permettent à ce titre de renforcer la sécurité juridique du procédé.

Selon le risque, il est constaté en pratique que les signatures « simples » (pour les ordres les moins risqués) et avancées (pour les ordres plus critiques comme, à titre d’exemple, les déclarations de bénéficiaire sur les comptes d’assurance vie) sont le plus souvent mises en œuvre.

L’ordre signé et horodaté permet de se prémunir contre les risques identifiés plus haut en assurant :

- Un lien fort entre l’ordre passé et l’identité du signataire, dépendant du niveau de certificat choisi, pouvant aller jusqu’au niveau qualifié ;
- Une garantie d’intégrité de l’ordre passé, pouvant aller jusqu’à la présomption de fiabilité ;
- Une garantie sur la date du passage d’ordre, pouvant aller jusqu’à la présomption de fiabilité ;

Intérêt de l’exécution d’ordres à distance : permettre au titulaire du contrat de passer des ordres à effet immédiat, sans se déplacer, et sans papiers à remplir.

Problématiques spécifiques relatives au déploiement : La problématique de déploiement consiste principalement à réaliser un arbitrage entre le risque associé aux ordres et les contraintes associées au niveau de sécurité des moyens de signature. Dans le secteur bancaire ou des assurances, l’évaluation du risque doit prendre en compte les montants en jeu, mais aussi le risque potentiel associé au type de support financier.

La fréquence de passage des ordres constitue un élément de choix du moyen d’authentification. Lorsque les ordres sont fréquents, le titulaire appréciera un processus rapide d’authentification et de signature même si son enregistrement initial est contraignant. Si le titulaire passe des ordres de façon très exceptionnelle (agir sur un contrat d’assurance vie), un enregistrement complet à chaque ordre sera préférable.

Comme tous les autres sujets relatifs à la signature électronique, les contraintes liées à la validation de l’identité lors de l’enregistrement initial (face-à-face, présentation d’une pièce d’identité) et lors de chaque transaction (authentification) sont à prendre en compte par les métiers et leur impact doit être identifié. Cependant, ces contraintes, contrairement à d’autres cas d’usage (souscription en ligne...), peuvent être vues comme des éléments de sécurisation de la transaction et donner une image positive et rassurante.

2.4 Factures

Objet du cas d’usage : dématérialiser *fiscalement* le processus de facturation, par opposition à la dématérialisation « simple » (numérisation pour des besoins internes à une entreprise), dans laquelle la facture originale à destination des services fiscaux reste sous forme papier.

L’essentiel des cas d’usage porte sur les factures B2B (« e-invoice »), sur un périmètre national ou international, ce second cas posant des problèmes spécifiques. Le volume des factures B2G a connu un développement important ces dernières années, en raison des obligations particulières qui ont été introduites : la directive européenne 2014/55/UE

[UE_2014/55] du 16 avril 2014 a permis l'élaboration d'une norme européenne sur la facturation électronique et sa transposition en droit français, à imposer progressivement l'envoi de factures électroniques aux entreprises fournisseurs des services publics.

Secteur d'activité : tous les secteurs d'activité sont concernés, mais on observe une grande diversité dans les environnements métier et les pratiques. Le *Code général des impôts* (art. 289-VII) [IMPOTS_289] prévoit trois modes d'échange possibles, dont un seul mentionne explicitement la signature électronique ; le décret [IMPOTS_2013-350] précise les conditions d'émission, de signature et de stockage des factures dans ce cas.

Au niveau européen et international, les exigences sur la signature électronique des factures sont variables (signature qualifiée ou non, certificat de cachet ou de personne physique, nécessité d'horodater ou non...). Par exemple, l'Italie impose la facture électronique signée électroniquement depuis le 1er janvier 2019.

Populations visées : la facturation électronique n'a de sens que pour les entités soumises à la TVA et produisant ou recevant un grand nombre de factures (modèle « peu de certificats, beaucoup de signatures/cachets »). Comme mentionné ci-dessus, le contexte le plus courant est le B2B ou le B2G, les particuliers n'étant pas équipés ou habitués à recevoir des factures signées électroniquement.

Niveaux juridiques : le contexte juridique est encadré par la directive européenne de 2014 et par ses transpositions nationales. Le cas échéant, une facture doit répondre aux exigences du pays émetteur comme à celles du pays destinataire. Le règlement eIDAS a permis, en théorie, d'harmoniser les termes au niveau européen (voir ci-dessous).

Plusieurs pays, dont la France, requièrent l'utilisation d'un certificat qualifié (signature ou cachet). L'utilisation d'un certificat de cachet est à privilégier, lorsqu'il est autorisé, car plus adapté à la signature en masse de documents.

À ce jour, il n'existe pas d'exigence relative à l'utilisation d'un service de vérification qualifié (pour les factures entrantes), ni de conservation.

Intérêt de la facture électronique signée : indépendamment du choix du mode d'échange retenu pour la dématérialisation des factures, la dématérialisation permet de réduire les coûts de traitement des factures (entrantes et sortantes), de lutter contre la fraude, de réduire les contestations et les délais de paiement. Le déploiement de la dématérialisation des factures est facilité par le fait qu'elle se place en fin ou en début (factures sortantes ou entrantes) de chaîne de traitement métier et l'existence de normes bien maîtrisées par les logiciels (format de documents et de signature standardisés).

En France, l'utilisation d'une signature électronique peut permettre de s'affranchir d'avoir à maintenir une « piste d'audit fiable ».

Volumétrie existante / cible :

Nombre de factures électroniques en 2017 (estimation), en milliards :

Contexte	Europe	Amérique du Sud	Amérique du Nord	Zone Asie-Pacifique
B2C	4	6	4	2
B2B/B2G	5	4	4	2

Source : E-Invoicing / E-Billing, Significant market transition lies ahead, étude Billentis, 2017

D'après des sondages effectués en 2016 en Autriche, Estonie, Allemagne, Espagne, Angleterre et USA, les factures PDF signées représentent 70% des factures électroniques B2B.

Gains réalisés : les bénéfices que l'on peut attendre de la mise en œuvre d'un processus de facturation électronique portent sur les aspects suivants :

- Réduction des coûts de traitement ;
- Réduction de l'impact environnemental (papier) ;
- Réduction des temps de traitement et de déclaration ;
- Amélioration de la traçabilité ;
- Conformité réglementaire.

À titre d'exemple, selon le *Worldwide electronic invoicing survey* (EY, 2018), en France, en 2016 :

	Papier	Électronique
Coût de traitement d'une facture sortante	7 €	0,3 €
Temps de traitement d'une facture (jours)	15	3
Nombre de factures traitées annuellement par ETP	6 000	90 000

Problématiques spécifiques relatives au déploiement :

Dès que le déploiement concerne un nombre important d'interlocuteurs, en particulier à l'international, il devient vite avantageux de s'appuyer sur un mandataire en mode SaaS, pour ainsi éviter d'être confronté aux spécificités relatives à la forme des factures ou aux types de signatures et cachets de chaque pays.

Indépendamment des obligations légales spécifiques, l'horodatage est recommandé pour sécuriser la transaction et également servir d'élément de preuve supplémentaire pour garantir la date de la transaction et ainsi lutter contre la fraude.

Types de certificats mis en œuvre :

Par exemple, en France, le *Code des impôts* requiert une « signature électronique avancée fondée sur un certificat qualifié et créée par un dispositif sécurisé de création de signature », ce qui est presque la définition d'une signature électronique qualifiée au sens d'eIDAS, mais le *Bulletin officiel des impôts* (BOI-TVA-DECLA-30-20-30-30-20131018) admet quant à lui les factures électroniques assorties d'une « signature électronique ou d'un cachet serveur » effectuées à l'aide d'un certificat RGS de niveau « deux étoiles » comme « équivalentes à une signature qualifiée ».

2.5 Contrats de travail

Objet du cas d'usage : la signature de contrat de travail à distance concerne tous les secteurs d'activités, mais principalement à ce jour ceux ayant un recours régulier à des intérimaires (travail temporaire). La signature dans ces cas particuliers est réalisée dans un contexte tripartite comprenant les donneurs d'ordres (communément appelés

Entreprise Utilisatrice), les agences d'intérim et les intérimaires. Le recours au travail temporaire conduit l'agence d'intérim à conclure deux contrats :

- Un contrat traitant de la relation contractuelle avec l'Entreprise Utilisatrice (**contrat de mise à disposition**) ;
- Un contrat avec le salarié intérimaire, qui fixe les conditions de travail et encadre la mission réalisée au sein de l'Entreprise Utilisatrice (**contrat de mission**).

Certaines organisations font également signer les contrats de travail de leurs collaborateurs salariés par voie électronique, mais elles sont peu nombreuses à ce jour.

Secteur d'activité : Le travail en intérim concerne toutes les branches d'activité, avec toutefois une forte prédominance des secteurs industriels (industrie et construction) et des services (tertiaire).



Les 5 premiers secteurs (sur 88), en volume d'emploi (en ETP) en 2015 (source : DARES)



Populations visées : Les salariés intérimaires sont, pour l'essentiel, des ouvriers qualifiés et non qualifiés. Pour les contrats de travail « salariés », tous les secteurs d'activités et tous les types de populations sont potentiellement visés.

Niveau(x) juridique atteint(s) : Le contexte juridique de la signature est encadré, au niveau européen, par le règlement eIDAS. La signature avancée est parfois recommandée en raison des risques juridiques spécifiques au domaine (voir ci-après), mais la signature simple reste possible et est mise en œuvre par certains opérateurs. Les risques juridiques portent plus sur la requalification du contrat que sur son annulation (non-répudiation), le niveau de signature n'est donc pas forcément un sujet.

Le droit français reconnaît les écrits électroniques selon les conditions de l'article 1366 du Code civil [CIVIL_1366]. Toutefois, certains pays imposent l'utilisation d'une signature qualifiée pour la signature des contrats de travail (par exemple, l'Allemagne).

Intérêt de la signature électronique des contrats de travail temporaire : il existe, pour les contrats de mise à disposition, des contraintes réglementaires portant à la fois sur le contenu et le délai de signature. Ces contrats doivent notamment être conclus avec l'Entreprise Utilisatrice par écrit, pour chaque salarié, et au plus tard dans les deux jours ouvrables suivant la mise à disposition (Article L. 1251-42 du Code du travail [TRAVAIL_1251-42]). L'absence d'écrit est susceptible de constituer un motif de requalification en CDI du contrat.

Les contrats de mission doivent, quant à eux, contenir toutes les mentions expressément prévues à l'article L. 1251-16 du Code du travail [TRAVAIL_1251-16], et être adressés au plus tard dans les deux jours ouvrables suivant la mise à disposition du salarié.

	<p>Signature à distance : état des lieux et bonnes pratiques</p>	
-----------------------------------------------------------------------------------	----------------------------------------------------------------------	-------------------------------------------------------------------------------------

La signature électronique est donc un facteur clé de conformité, en sus des gains de productivité évidents pour tout l'écosystème.

Volumétrie existante / cible : chaque année, environ 17 millions de contrats sont conclus en intérim (recensement DARES). Ce chiffre est relativement stable et oscille entre 16 et 17 millions depuis 2006.

Gains réalisés : les bénéfices que l'on peut attendre de la mise en œuvre d'un processus de signature électronique des contrats de travail temporaire portent sur les aspects suivants :

- Un gain de productivité ;
- Le respect de la réglementation ;
- La rapidité dans les échanges ;
- La suppression du papier ;
- La réduction des temps et des coûts de traitement ;
- La garantie de l'intégrité du document signé électroniquement.

Cinématique typique : du point de vue d'une agence, la cinématique est la suivante :

1. L'Entreprise Utilisatrice dépose des demandes de travail auprès de l'agence.
2. L'agence sélectionne les candidats et les soumet à l'Entreprise Utilisatrice.
3. En cas d'acceptation d'une candidature,
 - a. L'Entreprise Utilisatrice et l'agence signent le contrat de mise à disposition ;
 - b. Le salarié intérimaire et l'agence signent le contrat de mission.

Problématiques spécifiques relatives au déploiement : l'agence d'intérim est l'entité centrale de la relation tripartite. Étant signataire des deux contrats, elle peut équiper ses collaborateurs d'un ou plusieurs certificats électroniques (signature simple ou avancée), ou bien d'un cachet électronique.



Les personnes ponctuelles du processus sont l'Entreprise Utilisatrice et les personnels intérimaires, pour lesquels il n'est pas possible de supposer qu'ils sont équipés de moyens de créer une signature électronique. La signature électronique de ces parties nécessite alors de dérouler un processus d'enrôlement (vérification d'identité des signataires) afin de donner toute sa valeur légale à l'écrit électronique que constitue le contrat.

Lorsque des certificats sont émis au nom des signataires, l'agence d'intérim joue en général le rôle d'autorité d'enregistrement, *mais elle doit prendre soin de bien séparer ce rôle du reste du processus de contractualisation afin d'éviter tout soupçon de conflit d'intérêt.*

L'horodatage des contrats ou des signatures n'est pas strictement requis mais est généralement mis en œuvre pour démontrer simplement le respect des délais réglementaires de signature susmentionnés.

Types de certificats mis en œuvre : deux grandes familles de certificats sont utilisées :

- Des certificats de personne physique, générés à la volée suite à un processus d'enrôlement en ligne ou préalable (p. ex., l'enrôlement des intérimaires par les agences peut être réalisé en amont de la signature des contrats de mission) ;

	<p>Signature à distance : état des lieux et bonnes pratiques</p>	
-----------------------------------------------------------------------------------	------------------------------------------------------------------	-------------------------------------------------------------------------------------

- Des certificats de cachet (généralement émis pour l'agence d'intérim) servant à sceller les contrats, sur lesquels sont apposés les signatures simples des signataires (enrôlement en ligne ou préalable, aussi).

2.6 Feuille de présence à une formation professionnelle

Objet du cas d'usage : dans le cadre d'une formation professionnelle suivie par un salarié, une attestation de présence est généralement exigée par l'employeur afin de valider la formation d'un point de vue administratif.

Pour ce faire, il s'agit ici de fournir un service permettant à un prestataire de formation de saisir, signer en ligne et transmettre une attestation de présence.

Secteur d'activité : tous secteurs

Populations visées : les prestataires de formation sont principalement ciblés par ce cas d'usage ainsi que tout individu professionnel ou particulier suivant ladite formation.

Aucun équipement particulier n'est imposé pour les signataires.

Niveau(x) juridique atteint(s) : à ce jour, ce cas d'usage est peu mis en pratique. Un tel cas d'usage peut raisonnablement s'appuyer sur une signature simple voire avancée pour les cas nécessitant un contrôle renforcé de l'identité des signataires.

Intérêt de la signature à distance : la dématérialisation de l'attestation de présence présente un intérêt commun pour les quatre parties (*le fond de formation, le prestataire de formation, le salarié, l'employeur*) et permet ainsi de :

- s'assurer de l'identité du prestataire de formation ;
- réduire les délais de fourniture de l'attestation de présence ;
- tracer et fluidifier le processus de validation administrative de la formation ;
- conserver de manière sécurisée l'attestation de présence.

Volumétrie existante / cible : à ce jour, le prestataire de formation transmet un exemplaire papier de l'attestation de présence au fond de formation et un autre exemplaire à l'employeur sur une base mensuelle.



Gains réalisés : signature électronique d'un « *exemplaire* » unique mis à disposition de toutes les parties prenantes (*le fond de formation, le prestataire de formation, le salarié, l'employeur*).

Cinématique typique : sur une base mensuelle, le prestataire de formation produit l'attestation de présence puis la signe électroniquement (*ou appose un cachet électronique*). L'attestation de présence est envoyée par voie électronique au salarié qui doit également la signer. Une fois signée par les deux parties, l'attestation de présence est transmise à l'employeur et au fond de formation.

Problématiques spécifiques relatives au déploiement : besoin d'identification du signataire et de collecte / vérification de ses pièces d'identité, besoin d'intégration avec des SIs existants...

Le service d'horodatage est indispensable à un tel service de façon à prouver la date et l'heure des actions des différentes parties.

Types de certificats mis en œuvre : pour le prestataire de formation, émission d'un certificat de cachet. Pour le salarié, émission d'un certificat électronique au nom du salarié, le plus souvent produit « à la volée » (au moment de sa signature, et de validité éphémère),

	<p>Signature à distance : état des lieux et bonnes pratiques</p>	
-----------------------------------------------------------------------------------	------------------------------------------------------------------	-------------------------------------------------------------------------------------

ou signature simple au nom du prestataire de signature électronique et faisant apparaître le nom du signataire dans les propriétés de la signature électronique.

2.7 Réception de Lettres Recommandées Electroniques (LRE) qualifiées

Objet du cas d'usage : fournir un service en mobilité équivalent au service de recommandé papier traditionnel

Secteur d'activité : tous secteurs qui ont des activités qui nécessitent un équivalent au recommandé papier pour faire preuve

Populations visées : personnes morales et personnes physiques (sans limite)

Niveau(x) juridique atteint(s) : LRE qualifiée exclusivement, équivalent avec un recommandé papier

Prérequis juridique : pour les destinataires personnes physiques, il est nécessaire de recueillir le consentement.

Intérêt de l'usage à distance du service de confiance : la LRE présente la possibilité d'émettre et de recevoir des recommandés sans passer par un bureau physique de dépôt ou de retrait. Elle est disponible en retrait 24h/24 – 7j/7. Le destinataire a également capacité à retrouver son RAR pendant 1 an, conservé dans un environnement sécurisé. Un service de LRE est accessible depuis n'importe quel endroit, y compris pendant les périodes de congés ou de déplacements. La LRE présente des gains en termes de réactivité, d'instantanéité vis-à-vis du service. Elle garantit l'intégrité de la donnée, du contenu des documents transmis, pour éviter la fraude ou la détérioration, la falsification, du contenu des informations reçues.

Volumétrie existante / cible : le volume est faible à ce jour, au motif que les services qualifiés l'ont été récemment. A terme, il est nécessaire de distinguer les marchés B2B (déploiement envisageable à court-moyen terme) et B2C (à plus long terme sans doute, au motif qu'il faut recueillir le consentement d'une part, et attendre qu'il soit équipé de dispositifs d'authentification d'autre part)

Gains réalisés : les gains sont nombreux, et sont à différencier selon l'acteur visé :

- **Pour l'expéditeur :** les gains sont l'efficacité (car il est plus rapide, moins chronophage, de produire des LRE de façon automatisée à partir d'un SI et d'APIs plutôt que de le faire sous un format papier), le coût (comparativement au coût du recommandé papier),
- **Pour le destinataire :** les gains sont plus qualitatifs, tels qu'exposés ci-dessus dans les bénéfices.

Cinématique typique : l'expéditeur, client du service de LRE, s'authentifie avec une identité reconnue par le service et dépose sa LRE. Le service construit une preuve de dépôt et notifie le destinataire. Celui-ci dispose de 15 jours pour accepter (ou refuser) la LRE. Le destinataire s'authentifie auprès du service de LRE via une fonctionnalité de ce service ou par une identité acquise auprès d'un fournisseur d'identité reconnu par le service. Le service de LRE transmet la LRE après authentification du destinataire, et construit la preuve de réception pour l'expéditeur.

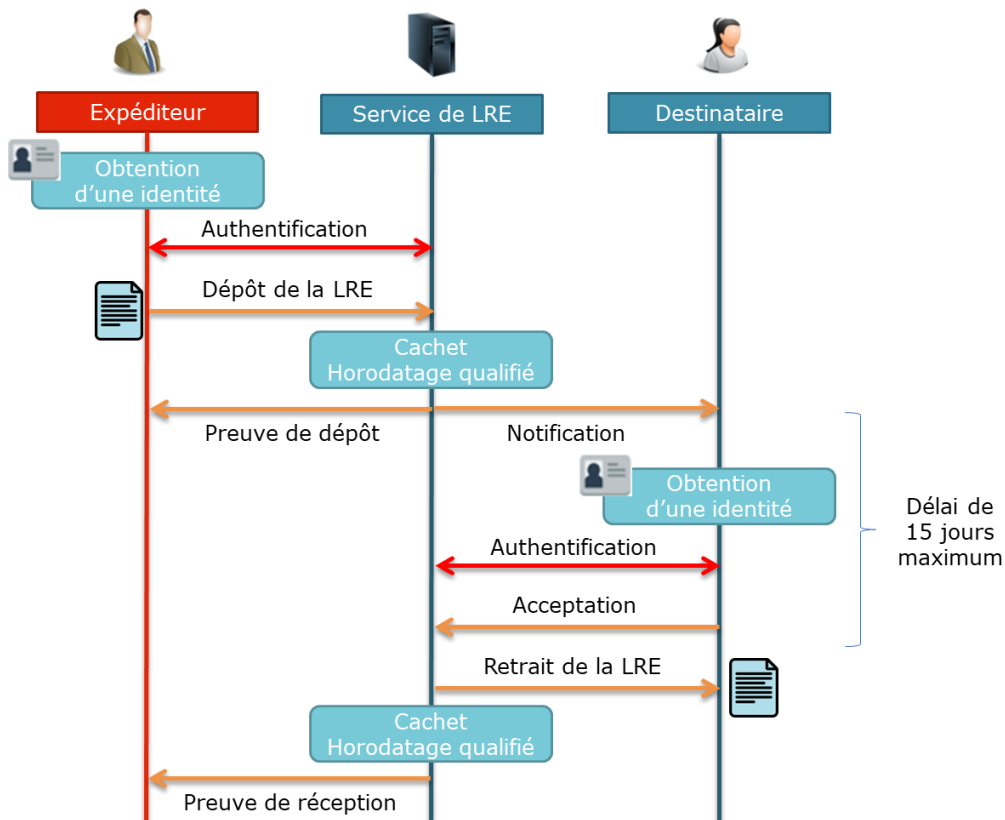


Figure 2 : Réception de Lettre Recommandée Electronique

Problématiques spécifiques relatives au déploiement : besoin d'identification de l'émetteur et du destinataire, par la collecte et la vérification de ses pièces d'identité (par le service de LRE lui-même ou par un fournisseur d'identité tiers), besoin d'un service d'horodatage (pour prouver la date et l'heure du dépôt, de l'acceptation ou du refus) et de cachet (pour prouver l'intégrité des données transmises), besoin d'équipement des destinataires (particuliers ou professionnels) en identités électroniques, besoin d'intégration du service dans le SI des partenaires.



Types d'identités mises en œuvre : plusieurs possibilités coexistent : des certificats qualifiés eIDAS ou RGS** sur support matériel (support logiciel pour un certificat serveur de personne morale), ou des identités eIDAS de niveau substantiel, un face à face physique étant requis pour l'expéditeur et un face à face à distance étant admis pour le destinataire.

Contraintes techniques spécifiques au cas d'usage : le service d'horodatage doit être qualifié, le cachet doit être un cachet avancé basé sur un HSM qualifié.

2.8 Attestations à distance

Objet du cas d'usage : générer, par un service en ligne, un document d'attestation dont l'authenticité pourra être vérifiée par un tiers. Les attestations peuvent être de diverses natures, et concernent à la fois les professionnels et les particuliers :

- Professionnels : Attestation de Responsabilité Civile et autres attestations d'assurance, attestation de conformité délivrée par un organisme d'audit, ...

	<p>Signature à distance : état des lieux et bonnes pratiques</p>	
-----------------------------------------------------------------------------------	----------------------------------------------------------------------	-------------------------------------------------------------------------------------

- Particuliers : Attestation d'assurance (responsabilité civile, habitation...), attestation d'emploi et/ou de salaire, attestation de diplôme, attestation de droit ou de couverture santé, attestation de détention d'un forfait de transport en commun...

Secteur d'activité : la production d'attestations concerne tous les secteurs d'activités, qu'ils soient marchands ou non marchands, étant donné la grande diversité des types d'attestation, et des besoins génériques tels que la demande d'attestations de la part d'un salarié vis-à-vis de son employeur.

Populations visées : les attestations sont émises aussi bien à des particuliers (clients, salariés, etc.) que des entreprises. Les destinataires in fine de ces attestations, qui en vérifient le contenu, sont eux-mêmes des particuliers (par exemple un propriétaire qui loue son bien et demande une attestation d'emploi du locataire), ou des entreprises (par exemple pour la vérification de couverture par une assurance d'un fournisseur).

Niveau(x) juridique atteint(s) : les attestations nativement numériques mettent en œuvre une signature ou un cachet simple, ou bien une signature ou un cachet avancé, au choix du fournisseur. La multiplication de cas de faux documents (par exemple produits par des particuliers pour l'obtention d'un logement ou d'un emploi) incite, indirectement, les producteurs de ces attestations à augmenter le niveau de sécurité (intégrité, authenticité) des documents produits.

Intérêt de l'attestation à distance : l'intérêt pour le demandeur est de pouvoir obtenir une attestation de façon immédiate, sans se déplacer et à tout moment. Pour le fournisseur de l'attestation, le service en ligne satisfait les exigences de simplicité et de rapidité des demandeurs, et élimine le coût de production et d'envoi d'une attestation sous forme papier. La garantie d'intégrité et d'authenticité de l'attestation électronique rassure le destinataire de celle-ci, et évite au fournisseur de l'attestation des sollicitations de vérification des informations ainsi que le ternissement de son image par la création facile de fausses attestations en son nom.

Volumétrie existante / cible : les attestations ont une durée de validité généralement courte (souvent un an maximum) et certaines sont demandées régulièrement, ce qui génère une demande régulière de la part de chaque entreprise et particulier. La dématérialisation des services bancaires, d'assurance et de ressources humaines fait augmenter chaque année ce besoin.



Gains réalisés : la mise en place d'une attestation à distance apporte des bénéfices immédiats à la fois au demandeur de l'attestation et à son producteur.

Pour le demandeur, l'attestation à distance permet :

- d'éviter un déplacement ou un appel téléphonique pour la demande,
- de pouvoir effectuer la demande 24h/24 7j/7,
- de gagner du temps en réceptionnant immédiatement son attestation,
- de pouvoir transmettre électroniquement et sans délai cette attestation au tiers à qui elle est destinée.

Pour le producteur de l'attestation, sa production par un service en ligne permet :

- d'automatiser entièrement la production de l'attestation (recherche des informations à inclure) et donc de libérer du temps pour ses collaborateurs,
- de supprimer les coûts d'impression et d'expédition de courriers papier,

	<p>Signature à distance : état des lieux et bonnes pratiques</p>	
-----------------------------------------------------------------------------------	----------------------------------------------------------------------	-------------------------------------------------------------------------------------

- de minimiser le temps de traitement de demandes de vérification des attestations grâce à la fiabilité de la signature électronique ou du cachet électronique inclus.

Cinématique typique : la production d'une attestation à distance suit un processus séquentiel simple :

1. le demandeur se connecte à l'espace en ligne de l'entité à laquelle il demande une attestation (une assurance, une mutuelle, son employeur...) et sollicite une attestation ;
2. le document d'attestation est produit immédiatement à partir des informations associées au demandeur en back-office, et ce document est revêtu d'un cachet électronique au nom de l'entité. La signature électronique par un collaborateur de l'entité est aussi possible mais augmente le délai de production et les coûts associés ;
3. le document signé est fourni au demandeur soit de façon synchrone par le service en ligne (téléchargement), soit de manière asynchrone par messagerie.
4. le demandeur transmet alors cette attestation, par ses propres moyens, au destinataire qui a requis ce document,
5. le destinataire final peut vérifier, grâce au cachet ou à la signature électronique, l'intégrité et l'authenticité des informations portées sur l'attestation.

Problématiques spécifiques relatives au déploiement : la production et la transmission de l'attestation ne posent pas de problème particulier puisque le demandeur a généralement déjà un accès à un site de l'entité qu'il sollicite. Le point d'attention porte sur la capacité du destinataire (professionnel ou particulier) à vérifier et à accorder sa confiance à l'attestation produite. Pour cela, il est recommandé de produire l'attestation au format PDF et de faire en sorte que le certificat utilisé soit reconnu par le lecteur d'Adobe (Adobe Reader). Ainsi, ce dernier affichera au destinataire un message lui précisant que la signature est valide, et devrait apporter la confiance attendue. Si l'attestation produite a pour vocation d'être imprimée afin d'être insérée dans un dossier papier, la création d'un Cachet Electronique Visible peut être envisagée en remplacement d'un cachet électronique (principe du CEV 2D-DOC défini par l'ANTS). Ce type de cachet doit être vérifiable par un service ou une application accessible librement aux destinataires de l'attestation.

Types de certificats mis en œuvre : il est recommandé d'utiliser un certificat émis par une Autorité de Certification (AC) reconnue par Adobe (référencement AATL – Adobe Authorized Trust List), par exemple qualifiée au sens eIDAS.

Contraintes techniques spécifiques au cas d'usage : le service de cachet (ou de signature électronique) peut être déployé en interne de l'entité productrice de l'attestation, ou produit sur un service SaaS proposé par un prestataire de service de confiance qualifié.

3 CONDITIONS DE MISE EN ŒUVRE DE LA SIGNATURE A DISTANCE EN FONCTION DES NIVEAUX DE SIGNATURE

3.1 Signature simple

Le règlement eIDAS présente la définition suivante pour la signature simple (ou signature électronique) : « des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique et que le signataire utilise pour signer ».

Cette définition n'impose pas vraiment de contrainte technique, ce qui laisse une grande liberté d'interprétation, et donc, de mise en œuvre. Il s'agit toutefois du niveau le plus faible de reconnaissance qui ne protège pas du risque lié au « vol » ou à la duplication des données d'authentification.

Ce niveau n'impose pas nécessairement le recours à un certificat électronique puisqu'il n'est pas attendu nécessairement une garantie sur l'identité du signataire ni sur l'intégrité des données. Cependant, afin que la signature simple apporte une réelle valeur ajoutée par rapport à des données non signées, elle est réalisée en utilisant un certificat électronique :

- établi au nom du signataire (le « porteur » du certificat), et donc identifiant celui-ci ;
- assurant l'intégrité des données signées, par les mécanismes de calcul d'empreinte et de signature cryptographique.

Toutefois, le niveau de garantie de l'identité du signataire est faible (par exemple uniquement déclaratif) et son authentification au déclenchement de la signature repose sur des moyens basiques (par exemple la transmission d'un code par email).



Ce niveau de signature est souvent mis en œuvre via la génération de certificats éphémères à usage unique liés à une seule transaction de signature. Chaque transaction de signature implique alors la génération d'un nouveau certificat de signature lié au signataire.

3.2 Signature avancée

Le règlement eIDAS définit la signature électronique avancée de la manière suivante : « une signature électronique qui satisfait aux exigences énoncées à l'article 26 », c'est-à-dire satisfaisant aux éléments ci-après :

- 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, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif; et
- être liée aux données associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable.

Ce niveau de signature impose implicitement le recours à un certificat électronique, à la fois pour garantir le lien avec le signataire (identité du signataire fournie dans le certificat de signature généré) et garantir l'intégrité des données signées. La signature électronique avancée ne nécessite pas règlementairement d'être horodatée par un service d'horodatage, mais il s'agit d'une bonne pratique.

	<p>Signature à distance : état des lieux et bonnes pratiques</p>	
-----------------------------------------------------------------------------------	------------------------------------------------------------------	-------------------------------------------------------------------------------------

En mobilité, toute la question tourne autour du « contrôle exclusif » des moyens de signature (vol du terminal, communications non-filaires, stockage distant de la clé privée, etc.), car les autres exigences sont universellement admises comme étant couvertes par l'utilisation d'un certificat et d'une bi-clé. Ce contrôle exclusif peut être garanti de multiples façons mais se ramène, au final, à évaluer la robustesse des mécanismes de contrôle d'accès à la clé privée de signature.

3.3 Signature qualifiée

Le règlement eIDAS définit la signature électronique qualifiée de la manière suivante : « une signature électronique avancée qui est créée à l'aide d'un dispositif de création de signature électronique qualifié, et qui repose sur un certificat qualifié de signature électronique ».

Le recours à un dispositif de création de signature électronique qualifié nécessite, à distance, l'utilisation d'un module cryptographique matériel (HSM) notifié QSCD (Qualified Security Cryptographic Device) auprès de la commission européenne. Les contraintes sous-jacentes résident dans les moyens d'authentification qu'il est possible de mettre en œuvre sur ce type de matériel de manière à garantir le même niveau de sécurité que celui lié à l'utilisation d'une puce cryptographique remise physiquement au porteur.

Ces mécanismes peuvent imposer à ce que :

- L'authentification du signataire pour utiliser sa clé privée de signature se fasse directement au niveau du HSM ;
- L'application de signature soit mise en œuvre directement dans l'environnement du HSM.



Même s'il n'y a aucune contrainte réglementaire, l'état de l'art préconise d'horodater une signature électronique qualifiée par un service d'horodatage qualifié, en cohérence avec le niveau de garantie de la signature.

3.4 Normes et standards applicables

La création d'une signature à distance fait intervenir différents domaines tels que :

- La délivrance des certificats ;
- La protection des clés privées de signature ;
- Les format et standard de la signature ;
- La création de signature ;
- L'audit des prestataires.

Pour tous ces domaines, plusieurs niveaux de garantie sont définis. Ces niveaux ont une terminologie distincte dans chacun des domaines, ce qui génère bien souvent des confusions sur la garantie globale offerte par la signature à distance.

	<p>Signature à distance : état des lieux et bonnes pratiques</p>	
-----------------------------------------------------------------------------------	------------------------------------------------------------------	-------------------------------------------------------------------------------------

3.4.1 La délivrance d'un certificat

Un certificat de signature contient les informations d'identité du signataire (nom et prénom d'une personne physique et/ou dénomination et identifiant d'une personne morale). C'est grâce à ce certificat, intégré dans un document signé, que l'on sait qui a signé ce document.

Le certificat de signature est délivré par une Autorité de Certification (AC), qui agit en tant que tiers de confiance, pour garantir l'authenticité de l'identité présente dans le certificat. Le point clé de la délivrance du certificat réside dans le niveau de confiance que l'on peut accorder à cette identité.



Ce niveau de confiance dépend des conditions dans lesquelles le certificat est délivré, c'est-à-dire d'un ensemble de mesures techniques et organisationnelle aboutissant à la génération du certificat. Par exemple :

- Le signataire a-t-il rencontré un représentant de l'Autorité de Certification en face à face pour obtenir le certificat ou a-t-il simplement transmis des documents ?
- Quelles sont les preuves apportées par le signataire pour prouver son identité à l'Autorité de Certification, a-t-il dû présenter un document officiel d'identité ?
- Comment la clé privée de signature, associée au certificat, est-elle remise au signataire : est-elle contenue dans un fichier ou bien dans un élément matériel (clé USB, carte à puce), est-elle transmise en ligne / par courrier ou bien remise en main propre, la clé privée et son conteneur sont-ils considérés sûrs d'un point de vue cryptographique ?

Pour décrire ces pratiques, l'entité qui gère une Autorité de Certification, appelée un Prestataire de Service de Certification électronique (PSCe), publie un document nommé « Politique de Certification » (PC). Ce document couvre l'ensemble du cycle de vie d'un certificat, présente l'organisation et les mesures de sécurité techniques appliquées. Selon le niveau de sécurité visé, les pratiques mises en œuvre sont plus ou moins contraignantes ou onéreuses. C'est ainsi qu'un PSCe peut proposer plusieurs offres de délivrance de certificats, et pilotera ainsi plusieurs AC associées chacune à sa PC.

Afin de clarifier le niveau de sécurité atteinte par une AC, autant pour les acquéreurs de certificats que pour les destinataires de documents signés, l'ETSI a défini plusieurs politiques de certification de sécurité croissante. Elles sont décrites dans la norme ETSI EN 319411, et l'on trouve ainsi pour des certificats de signature les niveaux :

- LCP (Lightweight Certificate Policy) : Le certificat est émis après contrôle d'une copie d'un document d'identité officiel, transmise sous forme papier ou électronique ;
- NCP (Normalized Certificate Policy) : Le certificat est émis après contrôle en face à face avec le porteur d'un document d'identité officiel original ;
- NCP+ (Extended Normalized Certificate Policy) : Le certificat est remis sous les mêmes conditions que la politique NCP, mais la clé privée de signature est stockée sur un support cryptographique matériel ;
- QCP (Qualified Certificate Policy) : Le certificat est remis sous des conditions proches de celles de la politique NCP (ou NCP+), mais les mesures de sécurité sont plus strictes ;
- QCP-n-qscd (Qualified Certificate Policy with QSCD) : Le certificat est remis sous les mêmes conditions que la politique QCP, la clé privée est stockée sur un matériel cryptographique qualifié au sens eIDAS.

	<p>Signature à distance : état des lieux et bonnes pratiques</p>	
-----------------------------------------------------------------------------------	------------------------------------------------------------------	-------------------------------------------------------------------------------------

3.4.2 La protection des clés privées

La fiabilité d'une signature repose sur le principe qu'une clé privée de signature est utilisée exclusivement par son propriétaire (porteur) légitime, identifié dans le certificat associé à cette clé privée.

Ainsi, une fois la clé privée générée, il faut garantir qu'elle ne sera jamais utilisée par un tiers, et en particulier :

- Que chaque création de signature soit précédée par une authentification du propriétaire de la clé privée. Un mot de passe (pour un conteneur logiciel), un code PIN (pour une carte à puce) voire une authentification biométrique (empreinte digitale sur un téléphone) sont typiquement nécessaires pour signer ;
- Que la clé privée ou son conteneur ne puissent pas facilement être dupliqués. La copie d'un fichier est aisée en cas d'accès au fichier, mais la clé privée est elle-même chiffrée par un mot de passe. Les cartes à puce ou les matériels cryptographiques permettent d'interdire, avec un très haut niveau de sécurité, la copie et l'accès illégitime à une clé.

Les exigences de sécurité pour les matériels cryptographiques d'un PSCE sont exposées dans le profil de protection CEN EN 419 221 [CEN]. Ces matériels peuvent protéger les clés privées des AC, ainsi que des clés privées de signataires, pour de la signature à distance, jusqu'au niveau de certificat QCP-n.

Lorsque le certificat émis pour le signataire n'est pas un certificat éphémère, les clés privées sont conservées pendant la durée de vie du certificat par l'opérateur du service de signature à distance. Des mesures de sécurité très strictes doivent être mises en œuvre pour assurer ce stockage qui est généralement assuré à l'extérieur du matériel cryptographique, et après chiffrement, à cause des capacités limitées de stockage de ces matériels. La réplication des clés, pour en assurer la disponibilité, peut être envisagée (avec des mesures supplémentaires) mais, pour en éviter les risques, il peut aussi être décidé de générer de nouvelles clés en cas de perte.

Pour pouvoir réaliser une signature qualifiée, le certificat doit être de niveau QCP-n-qscd et dans ce cas de la signature à distance, la solution cryptographique utilisée doit être conforme au profil de protection CEN EN 419 241 [CEN]. Ce profil définit deux niveaux de sécurité pour l'authentification du porteur du certificat (SCAL1 et SCAL2). Seul le second garantit une fiabilité suffisante pour prétendre créer une signature qualifiée.



3.4.3 Formats et standards de la signature

Le règlement eIDAS vise à favoriser la mise en place d'un marché européen numérique unique en facilitant l'utilisation transfrontalière de services en ligne. L'interopérabilité entre les services en est un élément fondamental, et elle passe par la définition de standards.

Les certificats sont tous conformes au standard technique IETF RFC 5280 [RFC5280]. Le contenu de certains attributs ou extensions de ces certificats sont fixés par les normes ETSI EN 319 412. Les certificats émis selon une politique de niveau QCP-n ou QCP-n-qscd sont clairement identifiés par un extension normalisée.

Les signatures électroniques avancées eIDAS doivent respecter des formats précis [ETSI], qui sont :

- XAdES (EN 319 132) : Format des signatures électroniques de documents XML ;
- PADES (EN 319 142) : Format des signatures électroniques de documents PDF ;

	<p>Signature à distance : état des lieux et bonnes pratiques</p>	
-----------------------------------------------------------------------------------	------------------------------------------------------------------	-------------------------------------------------------------------------------------

- CADES (EN 319 122) : Format des signatures électroniques de tout type de document, considérant celui-ci comme un bloc de données « binaire ».

Pour chacun de ces trois formats, plusieurs profils incrémentaux (en pratique, des niveaux de richesse des informations intégrées) sont définis :

- AdES-B ou B-B : Basic Baseline profile, où la signature intègre le certificat du signataire et quelques autres informations (heure du poste de signature, lieu de signature) ;
- AdES-T ou B-T : Timestamp Baseline profile, où la signature intègre un jeton d'horodatage certifiant l'heure de création de la signature ;
- AdES-LT ou B-LT : Long Term Baseline profile, où la signature intègre des informations facilitant la vérification de la signature au-delà de la durée de validité du certificat ;
- AdES-LTA ou B-LTA : Long Term Archiving Baseline profile, où la signature intègre des informations et des jetons d'horodatage successifs visant la validation sur le long terme.

Ces formats standard permettent de garantir des résultats homogènes dans la validation de la signature, quel que soit le prestataire assurant ce service.

Un protocole de création de signature à distance est défini dans la norme ETSI TS 119 432. Ce standard propose des architectures type pour chacun des deux niveaux de sécurité d'authentification du porteur du certificat (SCAL1 et SCAL2). Le protocole est décliné selon deux formats, XML et JSON.



3.4.4 La création de signature

Par nature, la création d'une signature à distance repose sur un prestataire de service de confiance qui maintient les clés privées de signature et en gère le contrôle d'accès. Ainsi, il est attendu que ce prestataire installe, opère et maintienne les dispositifs de création de signature en respectant les règles de l'art au niveau de sécurité attendu.

Le service de création de signature doit mettre œuvre les pratiques et les normes citées aux chapitres précédents. Le point clé de ce domaine est le niveau d'assurance du lien entre l'identité du signataire désigné dans le certificat de signature, et l'identité du porteur du moyen d'authentification utilisé pour activer la clé privée de signature associé à ce certificat.

Comme pour une Autorité de Certification, le fournisseur du service décrit ses pratiques dans une politique de création de signature à distance (SCP). Cette politique couvre le cycle de vie des clés de signature et les mesures de sécurité organisationnelles et techniques qui y sont relatives. L'ETSI a, ici aussi, défini plusieurs politiques de sécurité croissante pour clarifier les niveaux de garantie apportés par les différents services. Elles sont décrites dans la norme ETSI EN 119 431 :

- LSCP (Lightweight SSASC Policy) : La signature est créée avec peu de contraintes sur l'authentification du signataire et la protection de la clé privée, ce type de signature étant adapté à des cas où les risques sont faibles ;
- NSCP (Normalized SSASC Policy) : La création de la signature nécessite une authentification du signataire par un composant d'activation de niveau SCAL2, et la clé privée de signature doit être gérée dans un support sécurisé de création de signature ;

	<p>Signature à distance : état des lieux et bonnes pratiques</p>	
-----------------------------------------------------------------------------------	----------------------------------------------------------------------	-------------------------------------------------------------------------------------

- EUSCP (EU SSASC Policy) : La politique est de même niveau que NSCP, mais la signature doit reposer sur un dispositif de création de signature qualifié (QSCD).

Pour créer une signature qualifiée à distance, le service de création de signature devrait être conforme à la politique de niveau EUSCP et être réalisée avec un certificat qualifié.

3.4.5 L'audit des prestataires



Le règlement eIDAS prévoit la possibilité pour un prestataire de services de confiance de faire qualifier certains de ses services et de devenir ainsi un prestataire qualifié, gage de confiance vis-à-vis des utilisateurs de ces services. Que ce soit pour prétendre au niveau qualifié ou viser des niveaux de sécurité inférieurs, un prestataire peut faire évaluer sa conformité par rapport à des standards ETSI en relation avec le règlement eIDAS.

Ainsi, un prestataire de service de signature à distance pourra se faire auditer vis-à-vis de la norme EN 119 431, au niveau qu'il choisit. Cette norme s'appuie elle-même sur la norme ETSI EN 319 401, applicable à tous les opérateurs de service de confiance.

Le service de création de signature ne peut pas être qualifié en tant que tel, ni apparaître dans la liste de confiance européenne, comme peuvent l'être des services d'horodatage ou de délivrance de certificat. Cependant, un prestataire de service de signature à distance exploitant un QSCD aurait intérêt à faire auditer son service selon la politique EUSCP.

Les audits de conformité aux normes ETSI sont menés par des organismes d'audit, soumis eux-mêmes à la norme ETSI EN 319 403.

La qualification d'une offre de certificat ou d'un dispositif de création de signature est réservée à l'ANSSI, sur la base de procédures définies par l'ANSSI en conformité avec le règlement eIDAS [ANSSI_EIDAS].

	<p>Signature à distance : état des lieux et bonnes pratiques</p>	
-----------------------------------------------------------------------------------	----------------------------------------------------------------------	-------------------------------------------------------------------------------------

4 BONNES PRATIQUES DE MISE EN ŒUVRE DE LA SIGNATURE A DISTANCE

4.1 Bonnes pratiques organisationnelles

4.1.1 L'identification du signataire

Comme expliqué ci-dessus, le signataire est identifié dans une signature par un certificat électronique. Son identité est établie par le processus de délivrance de ce certificat. Il n'y a toutefois aucune spécificité au contexte de la signature à distance pour ce qui se rapporte au cycle de vie des certificats.

Cette identification doit bien évidemment se faire dans le respect des textes sur les données nominatives, en particulier du règlement n° 2016/679, dit règlement général sur la protection des données (RGPD).

Le niveau de garantie que l'on peut avoir sur l'identité du futur signataire joue un rôle important dans le niveau de signature associé.

On retrouve dans ces processus les possibilités suivantes :



- Vérification à distance des informations d'identité par un processus automatisé (reconnaissance automatique des informations présentes sur un justificatif d'identité : carte d'identité, passeport, carte de séjour, fiche d'imposition, ...) ;
- Vérification à distance des informations d'identité par un opérateur (vérification via téléphone, webcam par exemple) ;
- Vérification en face à face des informations d'identité avec un opérateur. Cela est considéré comme le niveau de vérification le plus élevé et le plus fiable.
- Récupération des informations d'identité du signataire sur la base d'une information sûre fournie par une source externe fiable (base de données du client, processus KYC, sources de données souveraines ...).

Dans le cadre de certificats éphémères, il peut être envisageable de ne pas vérifier l'identité du signataire à chaque transaction. Le processus de signature peut se baser sur des informations d'identité validées initialement (avant la première signature) et dont on considère leur fiabilité pendant un temps défini (souvent correspondant à 3 ans). Passé ce délai, il convient de réopérer une vérification formelle des informations d'identité.

4.1.2 L'authentification du signataire à la création de la signature

Suivant le processus de signature mis en œuvre, différents moyens sont envisageables pour authentifier le signataire et permettre le déclenchement in fine de la signature électronique :

- Génération d'un code à usage unique transmis au signataire au moment de la signature (généralement mis en œuvre pour l'utilisation de certificats éphémères) :
 - o Envoi d'un code SMS vers le numéro de mobile communiqué par le signataire. Ce mécanisme est reconnu aujourd'hui de moins en moins fiable et vise à être remplacé.
 - o Génération d'un code OTP sur une application mobile sur laquelle le signataire s'est préalablement enregistré. Ce mécanisme vise à remplacer le mécanisme précédent.

	<p>Signature à distance : état des lieux et bonnes pratiques</p>	
-----------------------------------------------------------------------------------	------------------------------------------------------------------	-------------------------------------------------------------------------------------

- Authentification du signataire sur la base d'un moyen d'authentification qui a été remis au signataire (généralement mis en œuvre pour l'utilisation de certificats pérennes) :
 - o Utilisation d'un certificat d'authentification remis ou non sur support cryptographique ;
 - o Utilisation d'un support physique type clé FIDO ;
 - o Utilisation d'un accès à un espace client (login / mot de passe, moyens d'authentification forte) ;
 - o Utilisation d'une application d'authentification forte tierce.

Dans le cas de la signature qualifiée (voire de la signature avancée sur la base d'un certificat qualifié), la mise en œuvre de ces mécanismes d'authentification nécessite de prendre en compte leur exécution dans l'environnement du HSM.

4.1.3 Recueil du consentement

Le consentement entre en jeu dans la constitution des éléments de preuves permettant finalement d'associer le document signé à l'ensemble de la transaction de signature.

Le consentement se matérialise à la fois :



- Sur les contenus présentés au signataire rendant l'opération de signature la moins ambiguë possible pour l'ensemble des parties ;
- Sur les éléments mettant en œuvre une interaction avec le signataire.

Le premier point doit permettre au signataire de comprendre le processus qui l'amène à signer et surtout savoir explicitement ce qu'il va signer. Pour cela il faut au minimum attester des informations suivantes :

- Les éléments de signature qui vont être mis en œuvre. Le certificat évidemment mais également les informations d'identité contenues dans son certificat peuvent être présentés visuellement au signataire. Par exemple informer l'utilisateur qu'il va signer en son nom propre (certificat particulier) ou bien en son nom dans le cadre de ses activités professionnelles (certificat entreprise) est un élément important. De même différencier l'utilisation d'un certificat de signature de personne physique d'un certificat cachet d'une personne morale amène un élément important dans le processus de recueil de consentement.
- Le contenu à signer. Cela paraît évident mais présenter le contenu à signer sous la forme d'un lien contenant le document à signer par rapport à une page présentant directement le contenu du document à signer n'amène pas la même certitude sur le consentement.
- D'autres informations éventuellement utiles à la compréhension de l'action de signature : le lieu de signature, l'horodatage de la signature, le recours à un prestataire produisant le certificat électronique (et qui ne serait pas le même que celui proposant le service de signature) ...

Le second point peut être couvert par la mise en œuvre de :

- Cases à cocher ;
- Textes à recopier ;
- Codes OTP à saisir ;
- Barres de défilement à dérouler ;

	<p>Signature à distance : état des lieux et bonnes pratiques</p>	
-----------------------------------------------------------------------------------	------------------------------------------------------------------	-------------------------------------------------------------------------------------

- ...

4.1.4 Compréhension du parcours par le signataire

L'objectif est de permettre aux différents acteurs (signataire notamment) d'identifier tous les éléments lui permettant de signer les documents souhaités en toute connaissance de cause. Cela implique notamment :

- L'affichage du document à signer ;
- L'affichage des Conditions Générales ;
- Eventuellement un rappel des informations qui seront portées dans le certificat ;
- Le rappel du moyen d'obtention du consentement (rappel du numéro de téléphone pour l'envoi SMS, rappel de l'adresse email ...) ;
- Protocoles de consentement.

Plusieurs éléments amènent des enjeux juridiques dans le processus de signature :

- Les éléments de constitution et d'utilisation du certificat électronique de signature ;
- Les éléments de signature en tant que telle.

De manière à s'assurer que le signataire a pleinement conscience de ces éléments, il convient de lui exposer ces derniers dans le processus de signature et idéalement avant la signature électronique.

Cela peut se matérialiser par la mise à disposition de Conditions Générales de Service de Signature visant à reprendre de manière synthétique les conditions de signature, les obligations du fournisseur et celles du signataire.

L'obtention du consentement du signataire peut prendre différentes formes :

- Une simple case à cocher avant le déclenchement de la signature ;
- La visualisation sur une page imposant la prise de connaissance ou la lecture du contenu ;
- L'envoi d'un code OTP par SMS pour déclencher la signature.

4.2 Bonnes pratiques techniques



4.2.1 Visualisation des informations signées

La visualisation des informations à signer viennent apporter un élément probant pour justifier le fait que le signataire était conscient de ce qu'on lui a soumis à signature.

Sur un poste fixe, la taille et la définition des écrans, la connexion réseau et les capacités des navigateurs (ou des applications) permettent d'assurer une consultation ergonomique pour le signataire.

En environnement mobile, la visualisation des informations à signer doit prendre en compte la diversité des environnements techniques envisageables et leurs contraintes potentielles. Des bonnes pratiques concernant ce cas de figure sont proposées ci-dessous.

Avant que le signataire ne puisse visualiser un document, encore faut-il qu'il soit transféré, stocké sur le terminal. Tant pour des raisons de bande passante que de mémoire disponible, il s'agit là d'une contrainte forte sur les documents signés.

	<p>Signature à distance : état des lieux et bonnes pratiques</p>	
-----------------------------------------------------------------------------------	----------------------------------------------------------------------	-------------------------------------------------------------------------------------

Remarquons que rien n'oblige, techniquement comme réglementairement, à ce que les données affichées soient les données signées. Ainsi, dans le cas de la signature d'un contrat au format PDF, on peut imaginer une solution qui présenterait au signataire le contenu de ce contrat sur le terminal, mais dans un format plus léger, plus facilement présentable par le terminal. Cette façon de procéder induit bien entendu un risque accru de contestation sur la fiabilité de l'affichage...

En définitive, il importe, dans le contexte de la signature en mobilité, de ne signer que des documents ou des informations que l'on est en capacité de voir de façon intelligible sur le terminal mobile.

4.2.2 Création de la signature électronique



Il s'agit ici de décrire comment la signature va être produite :

- Génération de la bi-clé de signature ;
- Génération du certificat ;
- Authentification pour l'accès à la clé privée ;
- Mise en œuvre du service de signature.

La bi-clé de signature doit être générée selon un algorithme cryptographique à l'état de l'art afin de garantir sa résistance aux attaques sur sa valeur. Aujourd'hui, les clés de signature ou de cachet sont le plus souvent des clés RSA 2048 bits.

Le support et les mécanismes de génération de la bi-clé constituent des critères primordiaux de sécurité. La clé peut être générée de façon logicielle en mémoire du serveur, ou dans un module cryptographique matériel (voir les standards applicables au §3.4.2). En mémoire, il faut veiller à ce que la valeur de la clé privée ne soit accessible qu'aux processus légitimes, et porter une attention particulière à la destruction sécurisée des valeurs une fois son utilisation terminée. La génération de la clé repose sur des aléas dont il faut s'assurer de la qualité en veillant à l'initialisation du générateur pseudo-aléatoire. Un HSM intègre le plus souvent un générateur d'aléa de bien meilleure qualité, basé sur des méthodes physiques, et évalué selon des normes de sécurité strictes. Le HSM est capable de protéger efficacement l'accès et la confidentialité des clés qu'il a générées, ainsi que de les détruire de façon sûre.

Le certificat de signature est construit à partir de la clé publique de signature, des informations d'identité du signataire et d'un gabarit préalablement établi. Dans le cas de la signature à distance, les certificats de signature sont encore le plus souvent des certificats générés au moment de la demande de signature (certificats à la volée), utilisés uniquement pour une transaction et d'une durée de vie très courte. Toutefois, certains services de signature et en particulier les services de signature qualifiée à distance se basent sur des certificats de longue durée de vie (typiquement 3 ans). Ceci permet au signataire de réaliser de nouvelles signatures en ayant simplement besoin de s'authentifier mais sans avoir à présenter de nouveau des documents d'identité. La contrepartie est que le prestataire de service doit mettre en œuvre des mesures de sécurité importantes pour garantir l'usage exclusif des clés de signature par leur porteur légitime. Dans le cas de signature simple, un certificat de cachet, émis au nom de l'entité avec qui le contrat est signé par exemple, peut être suffisant pour garantir l'intégrité du document. Cette solution simple est applicable lorsque les risques sont estimés comme faibles.

	<p>Signature à distance : état des lieux et bonnes pratiques</p>	
-----------------------------------------------------------------------------------	------------------------------------------------------------------	-------------------------------------------------------------------------------------

Avant de créer la signature et d'utiliser la clé privée, le service de signature à distance doit s'assurer que la clé est bien utilisée pour le signataire identifié dans le certificat correspondant. Les bonnes pratiques de l'authentification sont décrites ci-dessus au §4.1.2. Les preuves (traces d'exécution) de cette authentification doivent être conservées pour, en cas de contestation, fournir des éléments tangibles de l'implication du signataire (par exemple les traces liées à un code à usage unique par SMS). Les standards applicables à la création de signature à distance définissent des niveaux de sécurité relatifs à cette authentification (voir au §3.4.4).



La clé privée de signature, une fois activée par l'authentification du signataire, est utilisée en pratique pour signer une empreinte cryptographique du document signé. Le calcul de cette empreinte est fait selon les règles du format de signature (voir au §3.4.3). Le serveur de signature est chargé de ce calcul et du formatage du document signé. Ce serveur est de façon générale l'élément central de l'architecture. Il interagit avec le signataire pour lui présenter le document à signer et l'authentifier, génère ou demande la génération de la bi-clé de signature, sollicite une IGC pour obtenir le certificat, et enfin crée et formate la signature. La gestion de la clé privée doit être réalisée au plus près du matériel cryptographique, ainsi que l'authentification du signataire pour les signatures les plus sécurisées. La norme CEN 419 241 est dédiée à ces problématiques (voir §3.4.2 et §5).

4.2.3 La maîtrise de l'environnement logiciel et matériel

Le signataire utilise son équipement personnel ou professionnel pour interagir avec le service de signature à distance. Cet environnement peut présenter des vulnérabilités impactant la sécurité de la création de la signature à distance (interception de données d'identité ou d'authentification par exemple).

Même si l'on doit toujours conseiller aux utilisateurs de veiller à la sécurité de leurs propres appareils (antivirus, installation d'application d'éditeurs de confiance...), ceci ne peut pas être imposé en pratique aux signataires, surtout s'ils ne sont pas professionnels. L'opérateur du service de signature doit au minimum assurer la confidentialité des échanges par le chiffrement TLS des communications, vérifier l'intégrité des données reçues de la part des signataires et privilégier, autant que possible, des moyens d'authentification du signataire robustes (non rejouables par exemple). Le fournisseur du service de signature assure aussi la sécurité de ses propres plateformes, en suivant des standards comme les normes ISO 27k, les normes ETSI (EN 319 401) ou même le guide d'hygiène [HYGIENE] de l'ANSSI imposé pour les prestataires qualifiés.

Il existe aussi des risques plus spécifiquement liés aux environnements mobiles : les terminaux sont, le plus souvent, des plates-formes « ouvertes ». L'utilisateur peut y installer des applications dont l'origine n'est pas forcément sûre et qui peuvent interférer avec l'application de visualisation (voire la remplacer). Sur cette question, par exemple, l'ETSI évoque la nécessité d'avoir des « interfaces graphiques (écrans) infalsifiables », mais il n'existe rien de concret à l'heure actuelle. La question se pose aussi en ce qui concerne la confidentialité des données (code PIN, mot de passe) saisies sur le terminal, à cause de la présence potentiels de logiciels espions tels que les « keylogger » qui interceptent les données saisies par l'utilisateur.

	<p>Signature à distance : état des lieux et bonnes pratiques</p>	
-----------------------------------------------------------------------------------	----------------------------------------------------------------------	-------------------------------------------------------------------------------------

4.2.4 Gestion des preuves (création, conservation, restitution, contenu des preuves)

La validité des signatures à terme repose aussi sur la mise en œuvre d'un dossier de preuve. Celui-ci est en particulier utile pour renforcer la qualité de la défense juridique en cas de contentieux sur des signatures simples, avancées ou même qualifiées.

Le dossier de preuve doit contenir un ensemble de traces et de données produites durant le processus de signatures (fichiers de log, réponse à un challenge envoyé au signataire pour l'authentifier, etc.). Les normes ETSI relatives à la délivrance de certificats (ETSI EN 319 411) listent les informations à conserver, dont :

- Les informations d'enregistrement du porteur du certificat (preuves d'identité fournies) ;
- Les événements du cycle de vie de la bi-clé et du certificat ;
- Les traces d'acceptation des conditions générales d'utilisation du certificat, et du certificat lui-même ;
- Les procédures suivies pour la délivrance du certificat.

Le service de signature doit conserver aussi les preuves de :



- L'acceptation des conditions générales du service de signature ;
- La présentation du document au signataire (par exemple l'empreinte du document transmis, le moment de cette présentation, ...) ;
- Le consentement du signataire ;
- L'authentification du signataire pour l'utilisation de sa clé privée de signature ;
- De façon générale, les traces et preuves de réalisation du parcours de signature.

Il est également pertinent d'associer au dossier de preuve les éléments permettant de rejouer la transaction de signature.

Lorsque la durée de conservation des preuves et du document signé est très longue, il convient, en sus du document signé, de :

- Vérifier la validité initiale des signatures, puis à chaque événement impactant le document signé ou les preuves (fin de vie de certificats, pérennisation, conversions de format...) ;
- Documenter les modalités de stockage et tracer leurs évolutions ;
- Prévoir des opérations de pérennisation de la signature, afin de maintenir la validité et la robustesse des preuves (par exemple utiliser des algorithmes cryptographiques plus récents) ;
- Maintenir la lisibilité des documents en cas d'évolutions dans les formats standards.

Un dossier de preuve doit rester confidentiel, et accessible au besoin, sur toute sa durée de conservation. Pour les documents les plus sensibles, le recours à un système d'archivage électronique certifié constitue une garantie de sécurité appréciable. Chaque fournisseur de service de signature est responsable de mettre en place les mesures de sécurité appropriées aux risques et aux contraintes juridiques, réglementaires ou commerciales qui s'appliquent selon la nature des documents signés. Une procédure

	<p>Signature à distance : état des lieux et bonnes pratiques</p>	
-----------------------------------------------------------------------------------	----------------------------------------------------------------------	-------------------------------------------------------------------------------------

encadrée de restitution d'une archive doit être prévue dès le lancement du service, afin de pouvoir répondre aux demandes, et notamment aux réquisitions judiciaires.

4.2.5 Conformité au règlement sur la protection des données à caractère personnel (RGPD)

Un service de signature traite obligatoirement des données personnelles, notamment celles permettant de produire le certificat électronique de signature.

Dans ce cadre, le respect de la réglementation en matière de protection des données personnelles est à appliquer (règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE).

Comme prévu au titre du règlement, l'opérateur de service doit préciser le traitement qui est réalisé sur les données personnelles, au minimum :



- Les informations d'authentification au service et d'identification des signataires ;
- Les données commerciales et statistiques dans le cadre de l'offre de service souscrite auprès du fournisseur de service.

Toutes les données collectées doivent l'être uniquement si elles sont justifiées par un caractère obligatoire pour le fournisseur du service, qui doit en informer les usagers.

Quelques engagements minimums doivent également être respectés par le fournisseur :

- Garantie de confidentialité sur les données personnelles ;
- Conservation des données suivant une durée légitime et exclusivement pour permettre la réalisation de l'offre de service ;
- Informer les personnes concernées sur d'éventuels transferts et surtout mettre en place des clauses standards pour encadrer ces transferts ;
- Informer la personne concernée sur les actions du fournisseur relatives à la gestion de ses données personnelles ;
- Présenter le cadre de la sous-traitance le cas échéant.

Il est recommandé à ce que les conditions de traitement des données personnelles fassent partie intégrante des éléments d'information présentés au signataire.

	<p>Signature à distance : état des lieux et bonnes pratiques</p>	
-----------------------------------------------------------------------------------	------------------------------------------------------------------	-------------------------------------------------------------------------------------

5 DIFFERENTS SCENARIOS DE SIGNATURE A DISTANCE

L'objectif principal de la signature à distance est de permettre aux signataires d'accéder à leurs moyens de signature (clés privées et certificats associés) depuis n'importe quel environnement, à distance et y compris en mobilité.

Les moyens de signature sont ainsi hébergés sur un service accessible en ligne, et le signataire n'a besoin que d'un client pour y accéder et éventuellement d'un moyen d'authentification logiciel ou matériel pour déclencher la signature.

Aujourd'hui dans le cadre de la signature à distance, une norme européenne produite par le CEN (CEN 419 241) traite des mécanismes à mettre en œuvre au niveau du serveur de signature pour générer, stocker et utiliser la bi-clé du signataire. Cette norme n'est pas à ce jour applicable réglementairement mais apporte un niveau d'exigences important permettant à tout opérateur s'y conformant de garantir plusieurs mécanismes de sécurité, notamment les aspects de contrôle exclusif du signataire. Le recours à des services de signature à distance se conformant à cette norme permet de faciliter in fine la démonstration de l'atteinte de niveaux de signature conformes à eIDAS.

La signature à distance vise également, comme cela a été dit auparavant dans ce document, à couvrir l'ensemble des niveaux de signature prévus par le règlement eIDAS à savoir les niveaux de signature simple, avancée et qualifiée.

Pour prétendre à couvrir ces niveaux, il faut donc s'assurer que les exigences qui s'appliquent à chacune de ces niveaux restent couvertes en signature à distance.

Les paragraphes suivants présentent plusieurs scénarios de signature à distance :

- La signature simple sans vérification fiable d'identité ;
- La signature avancée avec vérification d'identité en ligne, en face à face ou à distance ;
- La signature qualifiée à distance, dont celle basée sur l'usage de moyens d'identification électronique notifiés.

Pour chacun de ces scénarios, les éléments comparatifs suivants sont établis :

- Schéma de principe ;
- Avantages ;
- Inconvénients.

5.1 Signature simple avec mécanisme d'intégrité

5.1.1 Principes

Dans ce scénario, on souhaite simplement obtenir une garantie sur le contenu du document signé. Il n'est ici pas nécessaire de faire signer directement le signataire, mais simplement obtenir son consentement à signer sur les données qui lui ont été présentées.

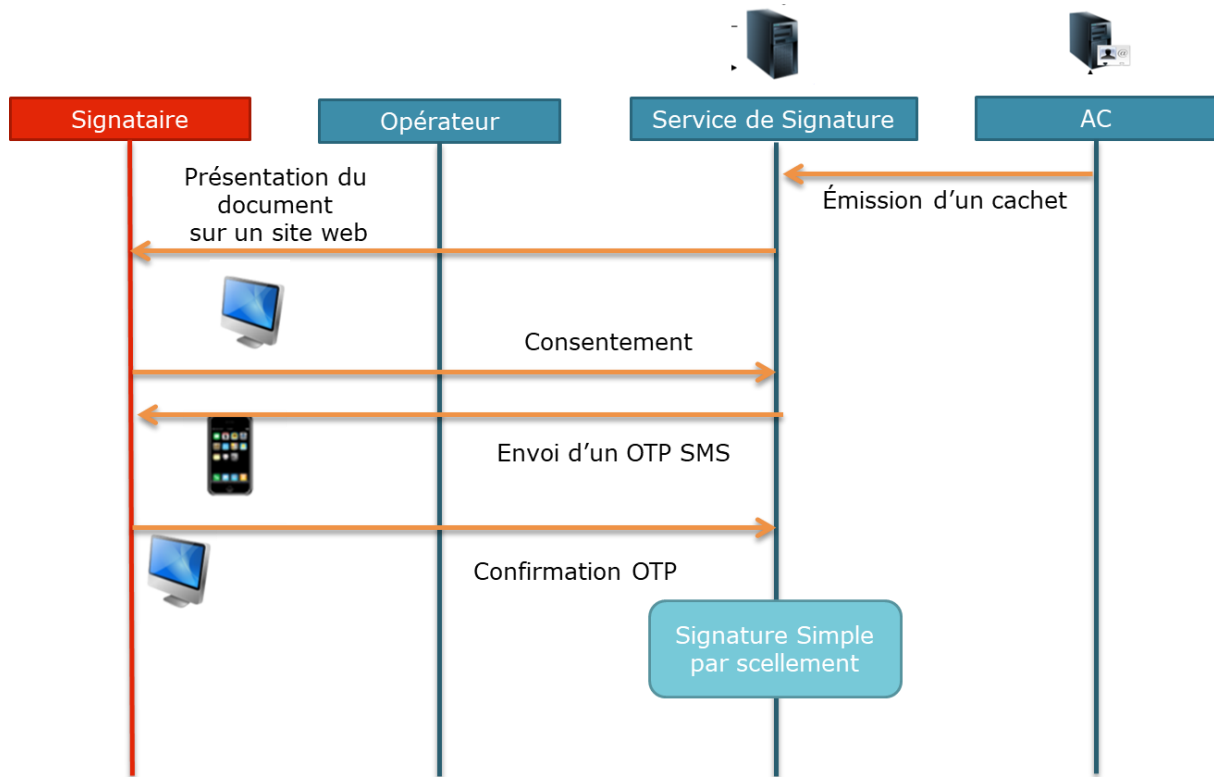


Figure 3 : Scénario simple de signature à distance

L'intégrité du document est alors le plus souvent portée par un certificat de scellement de l'application de signature. Ce certificat cachet est généralement un certificat durable.



L'authentification du signataire via un code OTP permet de tracer le consentement du signataire.

Visuellement sur le document signé il est possible d'ajouter dans le cartouche de signature des notions permettant d'associer le signataire à l'opération de signature en inscrivant par exemple « Document signé pour le compte de [prénom du signataire] [nom du signataire] »

5.1.2 Avantages & inconvénients

L'avantage principal de ce scénario est la mise en œuvre extrêmement facilitée. En effet l'objectif étant de garantir simplement l'intégrité du document signé, il n'est pas nécessaire d'authentifier et d'identifier formellement le signataire puisqu'il n'est pas nécessaire de générer un certificat de signature pour ce dernier. La mise en œuvre d'un authentifiant sur la base d'un code à usage unique (OTP) permet néanmoins d'associer le signataire au document signé, cela faisant l'objet d'une trace dans le dossier de preuve.

L'inconvénient réside alors dans la valeur juridique de cette transaction. Comme souvent si les mécanismes de signature mis en œuvre sont peu contraignants pour le signataire, le document signé devra être accompagné d'un ensemble d'éléments de preuve pour disposer d'une argumentation juridique suffisante. Enfin ce type de mécanisme ne garantissant pas l'identité du signataire, il reste alors facile pour la partie plaignante de contester la volonté de signer de la part du signataire.

	<p>Signature à distance : état des lieux et bonnes pratiques</p>	
-----------------------------------------------------------------------------------	----------------------------------------------------------------------	-------------------------------------------------------------------------------------

5.2 Signature sur la base d'un certificat généré à la volée

5.2.1 Préambule : le certificat généré à la volée

Dans de nombreuses situations, une personne amenée à signer électroniquement un document (par exemple une souscription en ligne) ne possède pas de certificat électronique pour le faire. Dans ce cas, un certificat est généré spécifiquement à cette occasion pour cette personne, juste au moment où la signature doit être créée. On parle donc de certificat généré à la volée, ou de certificat éphémère. En effet, ce certificat n'est utilisé que pour une unique transaction, et sa durée de vie est ainsi limitée à quelques minutes.

La génération de ce certificat est basée sur les informations d'identité connues du signataire (nom et prénom au minimum), et sur des clés cryptographiques générées dynamiquement, pour lui et pour cette signature, sur un serveur distant.

La signature à la volée ne préjuge pas de la qualité juridique de la signature ou de la durée de vie du certificat : la signature réalisée peut être simple, avancée ou qualifiée selon les mesures de sécurité adoptées dans le parcours de signature, et le certificat est en général éphémère mais peut aussi être pérenne.

5.2.2 Principes

Dans ce scénario, le signataire ne dispose pas directement de sa clé privée et du certificat associé. Ces éléments sont stockés chez un fournisseur de service Cloud de signature. L'opérateur génère, stocke et utilise la clé privée du signataire de manière sécurisée. L'usage de ces éléments est soumis au consentement du signataire.

Contrairement au scénario précédent, le signataire obtient ici un certificat portant son identité. Il signe alors en son nom.

Les éléments de signature sont générés de manière éphémère c'est-à-dire que la bi-clé et le certificat associé sont produits à chaque transaction de signature.

Lorsque le certificat est éphémère, l'identification du signataire permettant de déclencher la transaction de signature valide le lien entre le signataire, le certificat qui sera généré pour lui par le serveur pour le compte de cette transaction et le document à signer.

Le niveau de signature obtenue (simple, avancée ou éventuellement qualifiée) dépend alors à la fois des moyens matériels mis en œuvre par l'opérateur de signature mais également sur les processus (organisationnels ou techniques) mis en œuvre pour valider l'identité du signataire, et ce **pour chaque transaction de signature**.

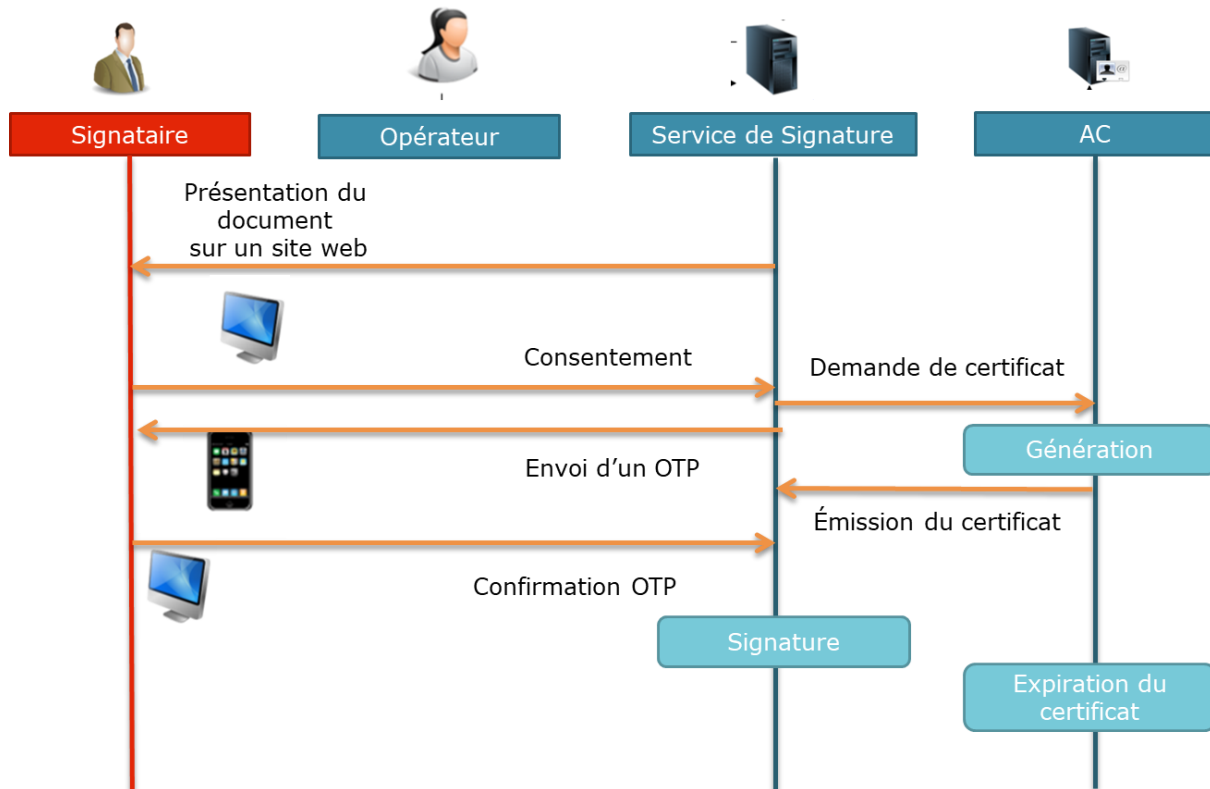


Figure 4 : Signature simple à la volée et à distance



La cinématique ci-dessus présente le cas d'une signature simple, mais la signature pourrait aussi être avancée (voire qualifiée) en ajoutant la vérification de document d'identité en ligne par exemple.

Au niveau de la protection de la clé privée, deux modèles peuvent être envisageables :

- Génération et utilisation dans un environnement matériel sécurisé (HSM). Les garanties de confidentialité et d'intégrité proposées nativement par ce type d'équipements sont alors apportées pour la protection de la clé privée de signature du signataire.
- Génération et utilisation de la clé privée en mémoire du serveur de signature. Les éléments de sécurité associés à la clé privée dépendent ici du niveau de sécurité de l'application de signature. Pour un opérateur de signature, il convient alors dans ce cadre de démontrer que les garanties de confidentialité et d'intégrité sont bien maintenues par l'application de signature.

Le deuxième aspect à couvrir dans ce scénario est la garantie que la signature est bien déclenchée par le signataire légitime. Nous pouvons retrouver ici des notions comme la garantie certaine de l'identité du signataire, l'accès ou le contrôle exclusif par le signataire sur la bi-clé de signature. Il s'agit ici d'observer deux schémas possibles :

- Le signataire est le seul à disposer des moyens permettant l'accès à la clé privée. Il dispose alors généralement d'un moyen physique ou d'un code personnel lui permettant de s'authentifier auprès du service de signature.

	<p>Signature à distance : état des lieux et bonnes pratiques</p>	
-----------------------------------------------------------------------------------	------------------------------------------------------------------	-------------------------------------------------------------------------------------

- Les éléments permettant de déclencher la signature sont connus potentiellement par des tiers. On retrouve ici les codes générés par le service de signature et transmis au signataire au moment de la signature.

Enfin le dernier élément important dans ce scénario est que le certificat émis a une durée de vie très courte (quelques minutes). Cela permet du coup de garantir la sécurité autour de la clé de signature quant à son utilisation limitée à la transaction en cours.

5.2.3 Avantages et inconvénients

Le processus mis en œuvre ici consiste bien à délivrer un certificat de signature au nom du signataire pour permettre la signature des documents rattachés à la transaction en cours. En sus de l'intégrité des données signées il y a bien ici une notion formalisée de consentement du signataire à signer ainsi qu'une signature au nom de ce même signataire. Juridiquement la notion de non répudiation est prise en compte dans ce scénario contrairement à celui détaillé au chapitre précédent.

De plus la mise en œuvre reste assez simple dans le sens où aucun élément physique a été délivré au signataire pour qu'il puisse valider sa demande de signature. Permettant a priori de répondre aux exigences eIDAS de la signature avancée, ce processus rencontre quelques limitations.

La qualité des informations d'identification du signataire, nécessaires à l'établissement du certificat de signature, ne font ici l'objet d'aucun contrôle poussé. Une bonne pratique visant à demander puis conserver une copie d'un document d'identité dans le dossier de preuve pourra permettre d'avoir des éléments opposables a posteriori, en cas de besoin.

Techniquement également, les signatures reposant sur des certificats éphémères, il est recommandé de procéder à un horodatage électronique pour être en capacité de les vérifier plus tard.

5.3 Signature avancée avec vérification d'identité

5.3.1 Principes

Par rapport au scénario précédent, ce scénario vise à apporter des mesures de contrôle des informations d'identité. Le certificat est toujours généré à la volée et est donc lié à la transaction de signature.

Le signataire est invité à uploader une copie de son justificatif d'identité qui va faire l'objet d'un contrôle automatisé côté serveur de signature. Les informations présentes sur le justificatif d'identité sont alors validées par rapport aux informations d'identité fournies par le signataire dans le cadre de la transaction de signature. Le résultat de la validation d'identité fait l'objet d'un élément de trace dans le dossier de preuves. Si le contrôle est validé, le certificat est alors généré et mis en œuvre par le service de signature.

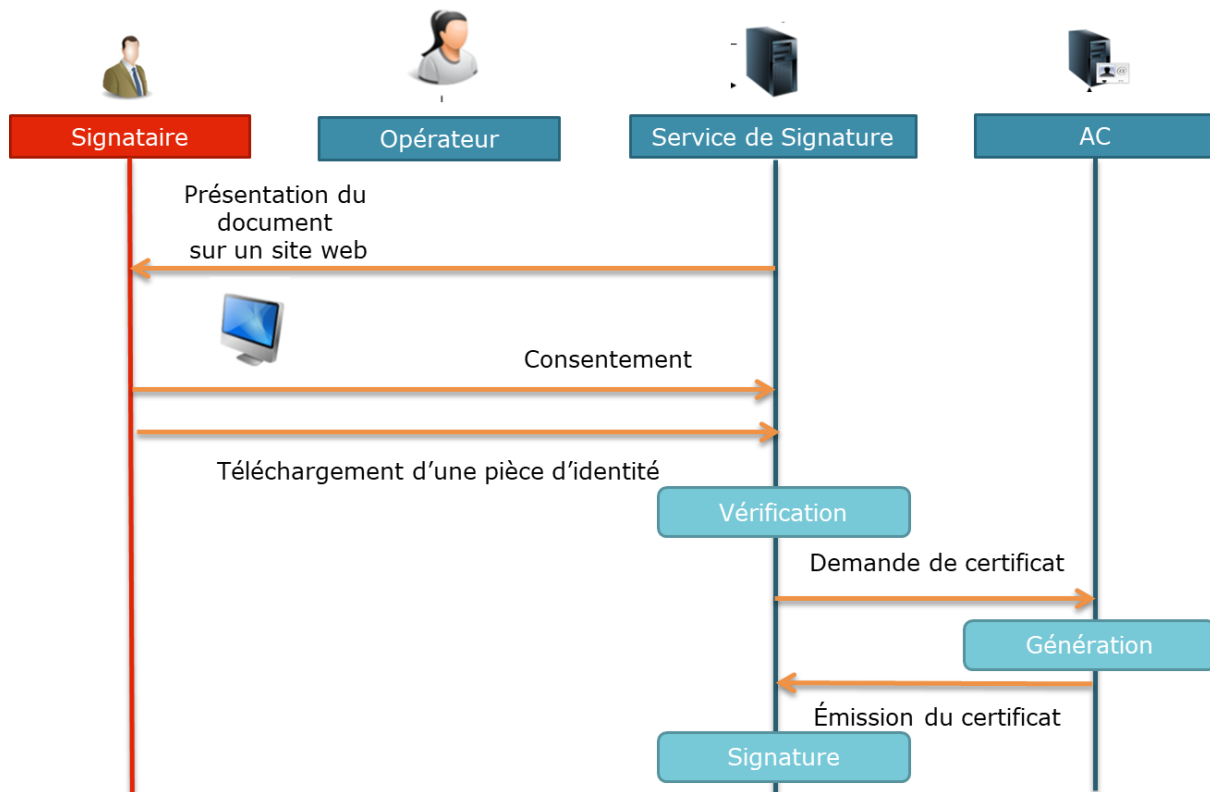


Figure 5 : Signature avancée avec vérification d'identité

5.3.2 Avantages et inconvénients

La valeur juridique de la signature électronique est renforcée ici par le fait que le certificat n'est produit qu'après la validation de la pièce d'identité. Cet élément probant de l'identité du signataire vient renforcer la garantie que l'identité du signataire est la bonne.

Pour associer un justificatif d'identité à la transaction, cela nécessite évidemment de fournir au futur signataire les moyens de soumettre une copie de son justificatif. Suivant les moyens mis en œuvre (appareil photo de téléphone portable par exemple), la qualité de la numérisation peut avoir un impact sur la capacité au serveur de signature de valider les informations d'identité. Enfin, dernier aspect à noter, ce mécanisme ne permet pas de s'assurer que la personne qui a soumis la pièce d'identité est bien la personne légitime. Ce scénario apporte juste une garantie sur le fait que le justificatif fourni est valide.

5.4 Signature avancée avec vérification en face à face physique

5.4.1 Principes

Nous rentrons ici dans des scénarios où la garantie sur l'identité du signataire est forte. Ce processus d'identification étant relativement coûteux, le certificat est généralement émis de manière durable.

Très adapté aux signatures de documents en agence avec un responsable commercial, il est possible dans ce cadre de disposer des conditions nécessaires permettant de produire des signatures avancées.

Le contrôle d'identité se fait dans le cadre d'un face à face physique avec un opérateur d'enregistrement. Via ce processus d'identification fiable, il est possible :

- De déclencher une opération de signature sur la base de certificats éphémères
- De permettre la génération d'un certificat durable dans un environnement sécurisé. Les moyens d'authentification permettant au signataire d'accéder et d'utiliser son certificat de signature peuvent alors lui être établis à ce moment.

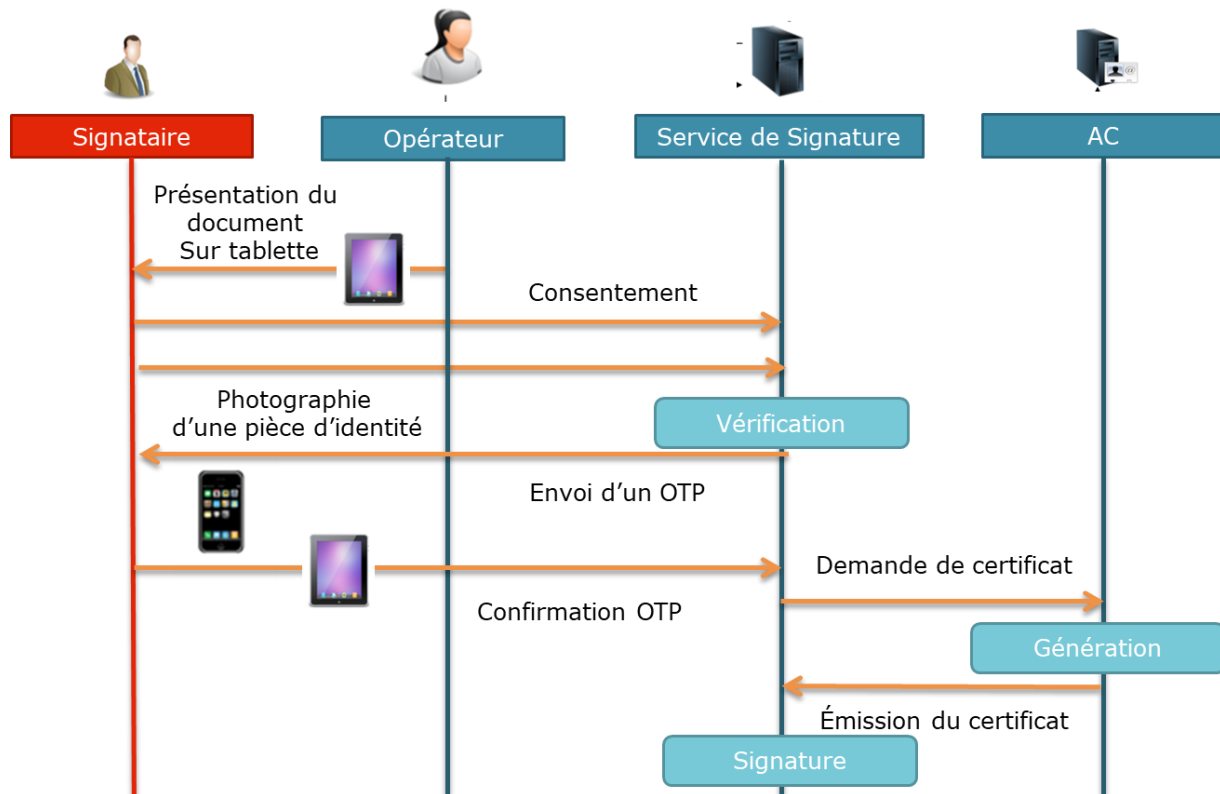


Figure 6: Signature avancée avec vérification d'identité en face à face physique

Le justificatif d'identité peut alors être numérisé et être ajouté au dossier de preuve. Dans le cas d'une signature sur base d'un certificat éphémère, la donnée d'activation peut se présenter sous la forme d'un code à usage unique. Dans le cas d'un certificat durable, le moyen d'authentification pourra être un moyen physique ou bien un moyen sous le contrôle exclusif du signataire (code PIN, mot de passe par exemple).

5.4.2 Avantages et inconvénients

Ce processus visant à apporter une garantie sur l'identification du signataire, il peut être associé à des processus de signature à base de certificats éphémères ou bien des processus de délivrance de certificats de signature durables et permettre, quel que soit le cas, de créer des signatures avancées.

Il est même possible de pouvoir disposer de certificats qualifiés dans ce cadre et ainsi de produire des signatures électroniques avancées sur base de certificats qualifiés.

L'inconvénient majeur reste alors la nécessité de faire un face à face, c'est-à-dire qu'il faut qu'organisationnellement la transaction de signature puisse se faire en présence d'un opérateur d'enregistrement capable de vérifier le justificatif d'identité.

5.5 Signature avancée avec vérification en face à face à distance

5.5.1 Principes

Ce scénario vise à atteindre les mêmes objectifs que le précédent, mais en dématérialisant le processus de face à face.

Les normes ETSI en support du règlement eIDAS autorise effectivement des processus de vérification d'identité dématérialisés dès l'instant où les procédés mis en œuvre garantissent le même niveau de contrôle qu'un face à face physique.

Cet aspect est important pour permettre la production de signatures avancées sur base de certificats qualifiés ou de signatures qualifiées.

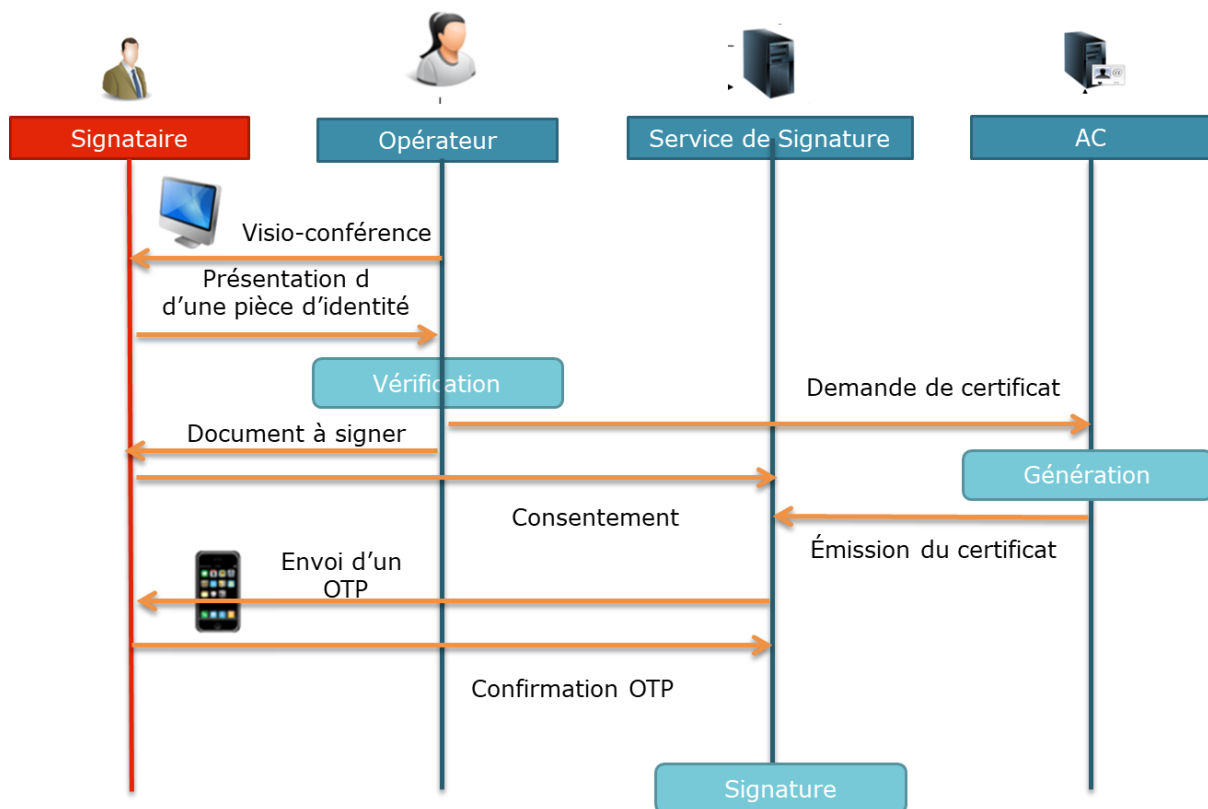




Figure 7 : Signature avancée avec vérification d'identité en face à face à distance

Des contraintes pèsent alors sur le système mis en œuvre pour réaliser le face à face « visio », notamment sur le niveau de sécurité des matériels utilisés. A ce jour, il n'y a pas de référentiels techniques précis, la validation du système mis en œuvre se fait alors au cas par cas, et doit être assurée par un organisme d'évaluation de la conformité eIDAS. Cette validation prend en compte le système utilisé pour le face à face mais dans le contexte d'usage de l'opérateur de signature. Cela veut dire que le même système utilisé

	Signature à distance : état des lieux et bonnes pratiques	
-----------------------------------------------------------------------------------	-----------------------------------------------------------	-------------------------------------------------------------------------------------

par un autre opérateur ou dans un autre processus doit également faire l'objet d'une évaluation.

5.5.2 Avantages et inconvénients

L'avantage principal dans ce scénario est de s'affranchir du face à face physique. Cela permet de centraliser les opérateurs d'enregistrement et de réaliser des équivalents face à face à distance.

Ce processus permet alors de disposer plus facilement d'une garantie certaine sur l'identité des signataires et ainsi produire a minima des signatures avancées à base de certificats qualifiés.

L'inconvénient majeur réside dans le côté novateur des procédés et il n'y a pas à ce jour de listes officielles de produits reconnus. Cela nécessite donc de traiter les procédés au cas par cas.

5.6 Signature qualifiée à distance

5.6.1 Principes

Dans ce scénario nous cherchons ici à obtenir une signature qualifiée à l'aide d'un certificat qualifié hébergé dans l'infrastructure de l'opérateur de signature.

Par rapport au scénario précédent, cela revient à générer, stocker et utiliser la bi-clé de signature (et le certificat associé) dans un environnement sécurisé QSCD côté serveur.

Il reste assez simple de mettre en œuvre un HSM qualifié QSCD pour générer et stocker la clé privée. La difficulté réside dans l'utilisation de cette clé et la garantie de contrôle exclusif par le signataire sur cette clé. Dans les faits, cela nécessite d'authentifier le signataire à chaque accès à la clé privée. Cette phase d'authentification nécessite qu'une partie du code de l'application de signature soit développée et mise en œuvre dans l'environnement du HSM. Cet aspect nécessite aussi de remettre au signataire un moyen d'authentification qui permet de s'assurer de son identité et de garantir ainsi le contrôle exclusif par le signataire sur sa bi-clé de signature.

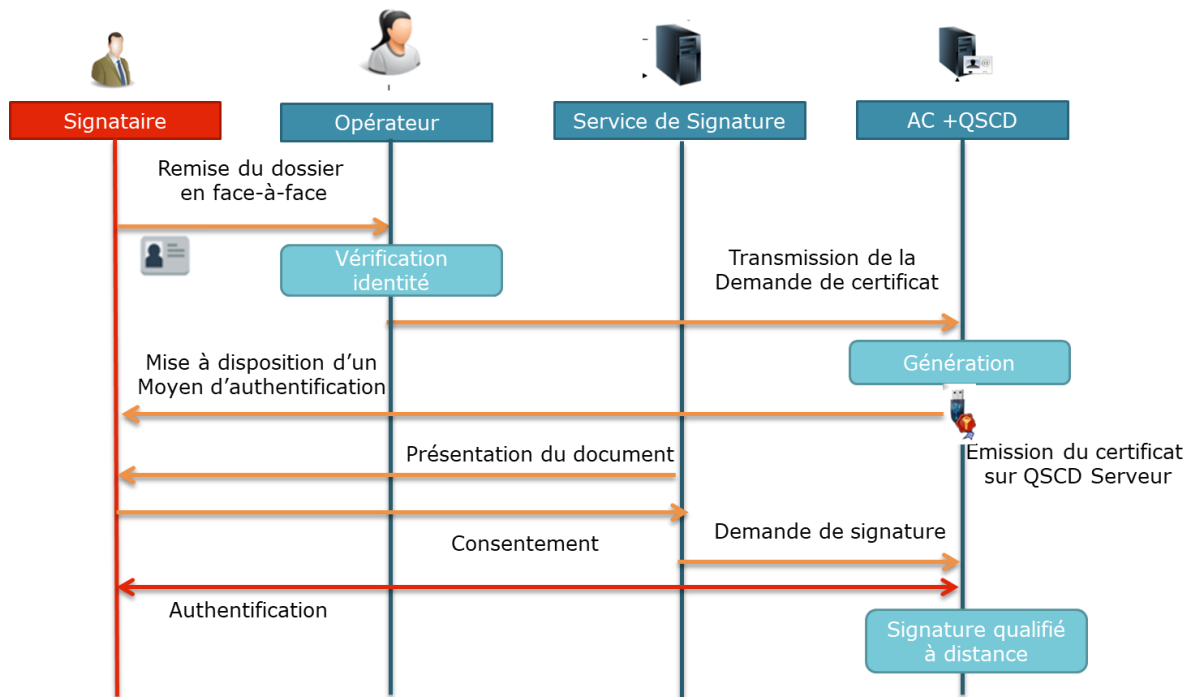


Figure 8 : Signature qualifiée à distance

5.6.2 Avantages et inconvénients

L'avantage ici est de permettre aux signataires de produire des signatures qualifiées avec une bi-clé gérée côté serveur.

Deux contraintes sont à retenir dans ce scénario. La première repose sur la qualification QSCD que doit avoir le HSM qui va générer, stocker et mettre en œuvre les clés de signature. A ce jour par exemple, la France n'a pas notifié de QSCD serveur. Il existe bien en Europe des QSCD serveurs notifiés mais pour un opérateur ou un Client final qui souhaiterait faire qualifier son service de confiance en France, cela pourrait poser une difficulté.

La seconde contrainte réside dans la mise en œuvre du QSCD serveur. En effet l'accès à la clé privée doit être couvert par un contrôle exclusif du signataire. Pour cela il faut que le moyen d'authentification remis au signataire soit d'un niveau au moins substantiel et ayant fait l'objet d'un face à face. Il faut donc ici aussi recourir à un moyen d'authentification compris dans un QSCD ayant fait l'objet d'une notification au niveau de la commission européenne. Outre le fait que cela nécessite de déployer ce moyen (probablement physique), il y a à ce jour une pénurie de moyens.

5.7 Signature électronique à partir d'eID notifiées

5.7.1 Principes

Comme évoqué dans le scénario précédent, l'authentification du signataire peut être produite sur la base d'un moyen d'identification électronique.

Il peut être alors utilisé des eID notifiées pour déclencher l'accès aux bi-clés. Pour la production d'une signature qualifiée, le règlement eIDAS prévoit que le moyen d'identification remis au signataire soit au moins du niveau substantiel.

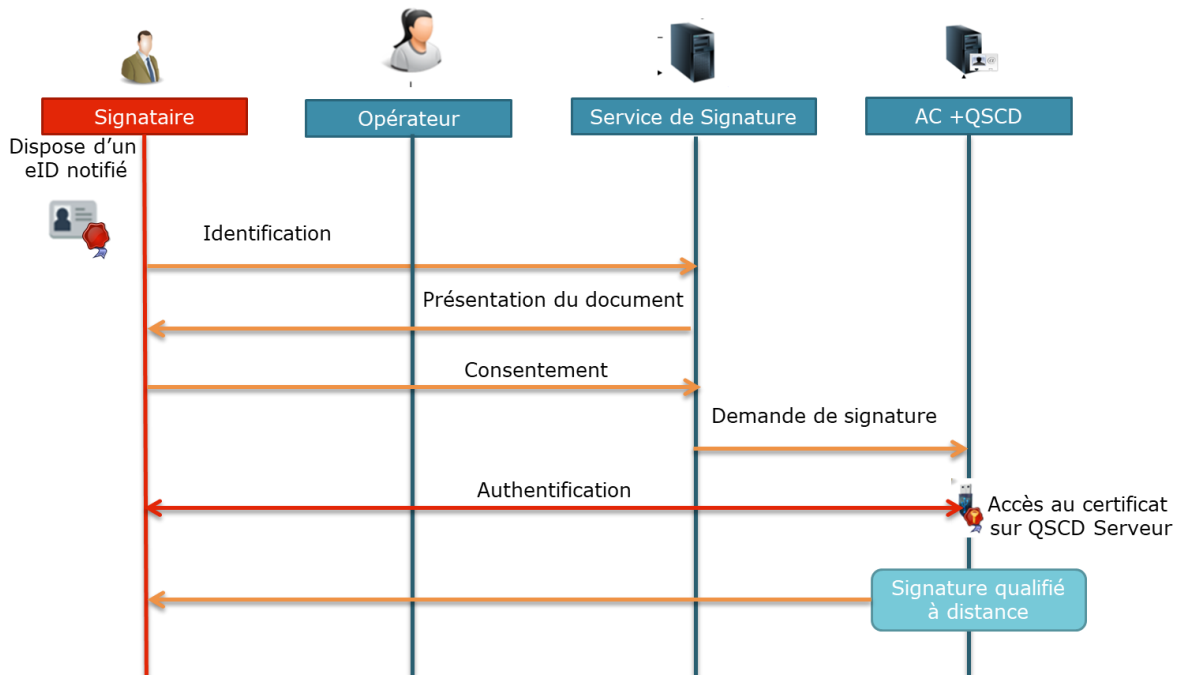


Figure 9 : Signature avec authentification par eID notifiée

5.7.2 Avantages et inconvénients

L'avantage est notable si le eID a été déployé auparavant car il permet de (ré)utiliser ce moyen pour toutes les transactions suivantes. Le recours par exemple à une carte d'identité électronique faciliterait la mise en œuvre d'une signature qualifiée.

Il faut également que l'application de signature (et donc le HSM associé) puisse fonctionner avec le eID concerné. Comme cela a été dit auparavant, il faut que la phase d'authentification soit intégrée à l'appli fonctionnant sur le HSM QSCD.

Comme pour le QSCD serveur, il n'y a à ce jour en France pas de moyens d'identification notifiés. De plus il est probable que le moyen d'identification notifié nécessite le déploiement d'un moyen physique et rende donc la mise en œuvre de ce genre de processus plus complexe.

5.8 Signature électronique à distance en environnement mobile

5.8.1 Principes

Ce scénario reprend des cinématiques décrites ci-dessus, mais en montrant comment elles peuvent être mises en œuvre dans un environnement entièrement mobile pour le signataire.

Dans un premier temps, le signataire s'enregistre auprès du service de signature avec son mobile, soit en transmettant des photos (prises avec son téléphone) de son document d'identité, soit via un face à face à distance. Le signataire est alors amené à initialiser un

moyen d'authentification forte sur son mobile, par exemple en téléchargeant et initialisant une application d'authentification. Le service de signature valide alors l'identité du signataire et peut demander un certificat de signature à une AC avec les informations recueillies (on peut aussi imaginer de générer un certificat à la volée au moment de la signature).

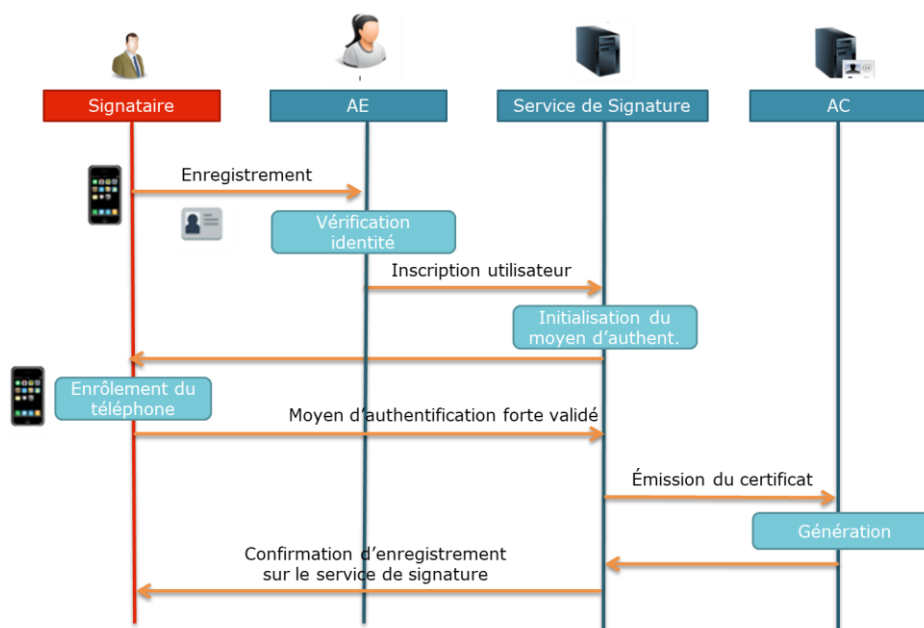


Figure 10 : Enregistrement du signataire en environnement mobile

Une fois ces étapes faites, le signataire dispose sur son environnement mobile d'un moyen d'authentification forte et d'un certificat de signature.

Quand le service de signature a besoin de faire signer ce signataire, il lui envoie une notification sur son téléphone. Lorsque le signataire est prêt à signer, il se connecte au portail de signature et s'authentifie par exemple par un login/mot de passe initialisé à l'enregistrement.

Après consultation du document et signification de son consentement, le signataire déclenche la création de la signature en utilisant le moyen d'authentification forte initialisé : par exemple il saisit un code PIN (ou utilise ses empreintes digitales) associé à une clé cryptographique locale de son application d'authentification. Le service de signature crée alors la signature avec le certificat préalablement généré à l'inscription (ou généré à la volée).

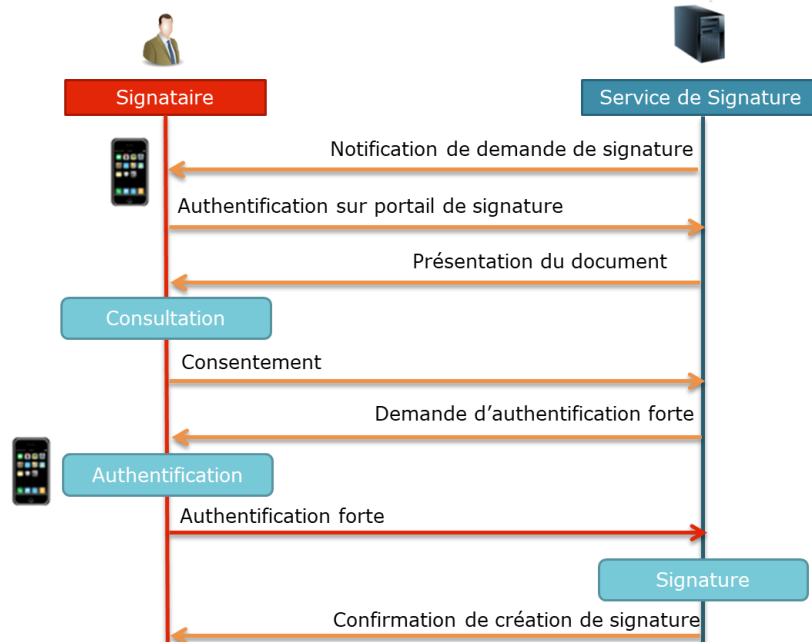


Figure 11 : Signature après authentification forte en environnement mobile

5.8.2 Avantages et inconvénients

Ce processus présente l'avantage pour le signataire de nécessiter uniquement un téléphone mobile pour la totalité du processus, et de pouvoir signer n'importe où et n'importe quand. Le processus est ainsi aussi bien adapté à une signature ponctuelle par un nouveau client particulier qu'à un professionnel qui doit signer régulièrement en mobilité.



Un inconvénient est de nécessiter le téléchargement d'une application sur le téléphone afin de disposer d'un moyen d'authentification forte et fiable (sinon on se retrouve dans le scénario décrit au §5.5 avec une authentification par OTP par exemple).

La valeur de la signature dépend de la fiabilité du processus de face à face à distance (voir au §5.5) mais la délivrance d'un certificat qualifié pourrait être atteinte. Si le service de signature à distance repose sur un QSCD à distance (voir au §5.6, il faut que l'application d'authentification forte soit reconnue fiable par l'ANSSI), alors la signature pourrait être une signature qualifiée.

6 ANNEXES

6.1 Textes règlementaires

[EIDAS]	Règlement (UE) 2014/910 du Parlement européen et du Conseil du 23 juillet 2014 https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32014R0910
[RE_2015_1502]	Règlement d'exécution (UE) 2015/1502 de la Commission du 8 septembre 2015 fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique du règlement eIDAS https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32015R1502
[GDPR]	Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 – Règlement Général de Protection des Données https://www.cnil.fr/fr/reglement-europeen-protection-donnees
[UE_2014/55]	directive européenne 2014/55/UE du 16 avril 2014 https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32014L0055&from=FR
[CIVIL_1366]	Article 1366 du Code civil https://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTIO00032042461&cidTexte=LEGITEXT000006070721&dateTexte=20161001
[IMPOTS_289]	Code général des impôts, article 289 https://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTIO00027517898&cidTexte=LEGITEXT000006069577&dateTexte=20130607
[IMPOTS_2013-350]	Décret n° 2013-350 du 25 avril 2013 https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000027356611&categorieLien=id
[TRAVAIL_1251-16]	Article L. 1251-16 du Code du travail https://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTIO00006901267&cidTexte=LEGITEXT000006072050&dateTexte=20190708&oldAction=rechCodeArticle&fastReqId=1005416216&nbResultRech=1
[TRAVAIL_1251-42]	Article L. 1251-42 du Code du travail https://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTIO00006901298&cidTexte=LEGITEXT000006072050&dateTexte=20190708&oldAction=rechCodeArticle&fastReqId=948166930&nbResultRech=1

	<p>Signature à distance : état des lieux et bonnes pratiques</p>	
-----------------------------------------------------------------------------------	----------------------------------------------------------------------	-------------------------------------------------------------------------------------

6.2 Normes et standards applicables

- [EN_319 401] ETSI EN 319 401 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
http://www.etsi.org/deliver/etsi_en/319400_319499/319401/02.01.01_60/en_319401v020101p.pdf
- [EN_319 411] ETSI EN 319 411-1 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
http://www.etsi.org/deliver/etsi_en/319400_319499/319401/02.01.01_60/en_319401v020101p.pdf
- [ETSI] Les normes ETSI sont publiées sur le portail de l'ETSI
<https://portal.etsi.org/Home.aspx>
et sont directement téléchargeables sous :
http://www.etsi.org/deliver/etsi_en
- [CEN] Les profils de protection CEN 419 221 et CEN 419 241 sont accessibles sous :
<https://standards.cen.eu>
- [RFC5280] PKI Certificate and CRL Profile
<https://www.ietf.org/rfc/rfc5280.txt>
- [ANSSI_PSCO] Prestataires de services de confiance qualifiés – Critères d'évaluation de la conformité au règlement eIDAS, Version 1.2 du 5 juillet 2017
https://www.ssi.gouv.fr/uploads/2017/01/eidas_psc-qualifies_v1.2_anssi.pdf
- [ANSSI_EIDAS] Référentiels d'exigences applicables à la qualification des prestataires de services de confiance
<https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-reglement-eidas/documents-publies-par-lanssi/>
- [RGS] Référentiel Général de Sécurité version 2.0 du 13 juin 2014
<https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/liste-des-documents-constitutifs-du-rgs-v-2-0/>
- [HYGIENE] Guide hygiène de l'ANSSI
<https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/>

6.3 Glossaire

ACPR	Autorité de Contrôle Prudentiel et de Résolution
AFAI	Association Française de l'Audit et du conseil Informatiques
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
B2B	Business To Business
B2C	Business to Customer
B2G	Business To Government
CAAdES	CMS Advanced Electronic Signature
eIDAS	electronic IDentification And trust Services
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
OTP	One Time Password
PAAdES	PDF Advanced Electronic Signature
QSCD	Qualified Signature Creation Device
RGPD	Règlement Général sur la Protection des Données
RGS	Référentiel Général de Sécurité
SCAL	Sole Control Assurance Level
XAdES	XML Advanced Electronic Signature