ClubPSCo

Le club des Prestataires de Services de Confiance

SIGNATURE EN MOBILITÉ : OBSTACLES ET SOLUTIONS

Version	Date	Description	Société
1.0	Mai 2014	Document pédagogique	SEALWeb - ClubPSCo

État du document	Classification
Pour diffusion	PUBLIC

SOMMAIRE

PREAMBULE

Ce document a été rédigé par l'association ClubPSCo dans l'objectif d'aider les responsables d'applications à identifier les contraintes et impacts des choix qui s'offrent à eux dans la mise en œuvre de la signature électronique en mobilité.

1.1 Qu'entend-on par « signature en mobilité » ?

Avec le succès des *smartphones* et le développement des offres mobiles (3G et 4G), l'accès à l'Internet s'effectue de plus en plus depuis un terminal mobile, qu'il s'agisse d'une tablette ou d'un téléphone. Par rapport à un ordinateur dit portable, ce terminal présente des caractéristiques particulières ayant un impact sur la mise en œuvre d'une signature électronique :

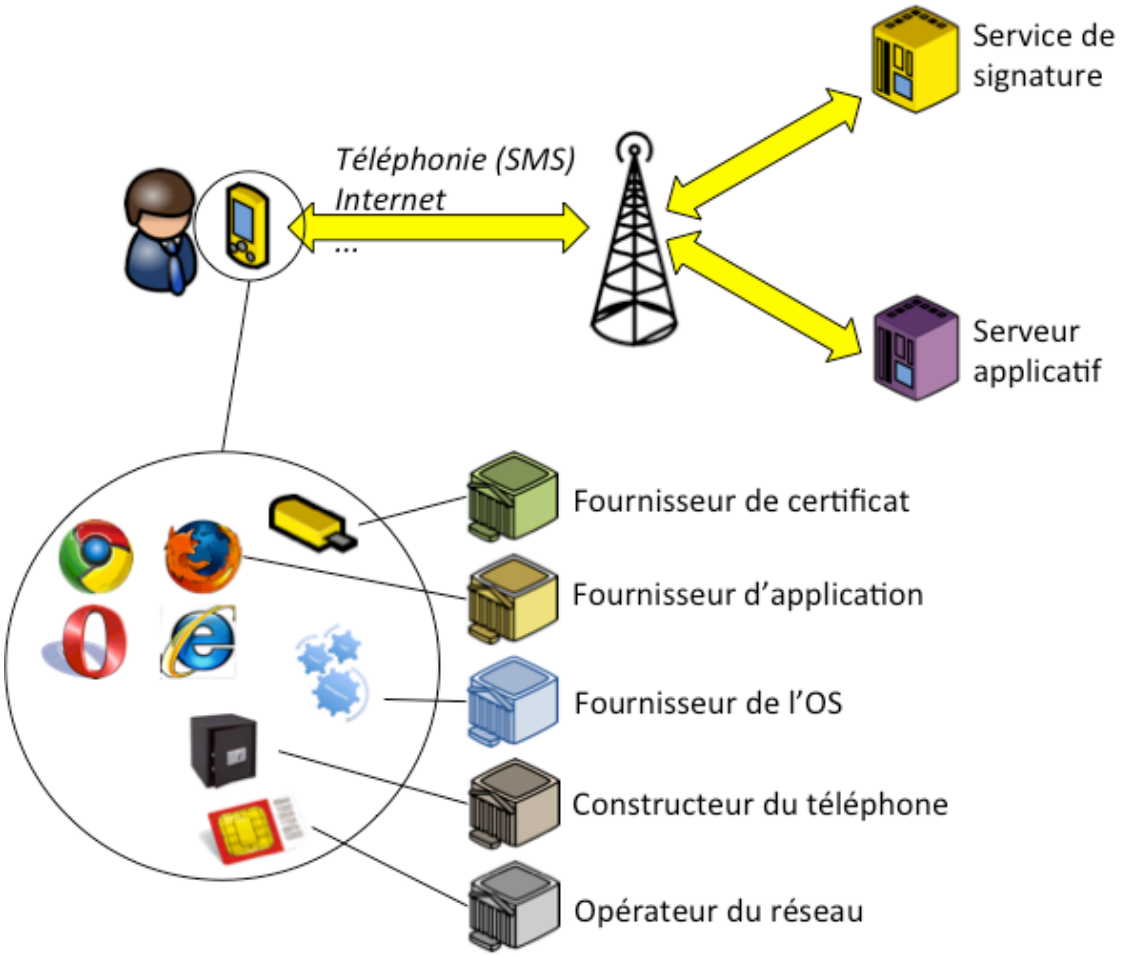
- un écran réduit, ce qui a son importance dans la visualisation des documents à signer.
- pas de clavier mécanique ; ces terminaux ne sont pas conçus pour saisir un grand nombre de signes. La saisie d'un mot de passe d'une vingtaine de caractères alphanumériques n'est pas concevable.
- caméra, écouteurs et micro sont présents en standard
- connectivité sans fil NFC ou Bluetooth
- des ressources limitées, en stockage et en traitement. La présence d'un environnement Java (JRE), par exemple, ne peut être assumée.
- Une grande diversité de plates-formes (matérielles et logicielles). Le marché est en perpétuelle évolution, les constructeurs se livrant une concurrence effrénée. Ce rythme de changement se retrouve dans celui des OS.
- Enfin, étant donné leur utilisation, ces terminaux sont plus souvent perdus, volés ou cassés que leurs homologues de bureau.

On parlera de « terminal mobile », et de « terminal » tout court lorsqu'aucune confusion n'est à craindre, pour désigner un tel équipement.

De plus, ces terminaux sont *personnels*. Là où un poste de travail fixe peut être partagé (poste multi-utilisateurs), les terminaux mobiles sont la propriété exclusive d'une seule personne, identifiée par la carte SIM et l'abonnement téléphonique dans le cas d'un *smartphone*. La signature en mobilité est donc une signature de personne physique, unitaire (pas de signature de masse).

1.2 Architecture globale

Le diagramme ci-dessous présente les principaux composants d'une solution de signature électronique sur ou depuis un terminal mobile.



1.2.1 Sur le terminal

Le terminal comporte des éléments matériels et des éléments logiciels. Au niveau matériel, hormis l'objet lui-même (écran, connectique, caméra/appareil photo), on identifie :

- *Secure element*

  Un *secure element* est un environnement sécurisé de stockage et d'exécution au sein d'une puce cryptographique (le plus souvent, une carte à puce). L'environnement assure un cloisonnement des applications et des fonctions de chiffrement, déchiffrement et signature cryptographiques. Cette notion vient du monde NFC[1].

- Carte SIM : fournie par l'opérateur de réseau téléphonique, elle peut aussi accueillir des données appartenant à l'utilisateur (certificat) ou des applications tierces (applets de signature, applications NFC,…).

Au niveau logiciel,

- Application de signature

[1] *Near Field Communication*

– Système d'exploitation (OS) : généralement préinstallé et limitant les droits de l'utilisateur, il peut avoir été altéré (*jailbreak*).

1.2.2 La clé privée de signature

Aucune hypothèse n'est faite au sujet du stockage de la clé privée de signature. Dans le cas d'un certificat logiciel, celle-ci peut résider dans la mémoire du terminal, dans la carte SIM ou dans un *secure element*. Un certificat matériel n'est toutefois pas exclu (clé USB, autre carte à puce), même si cette solution pose des problèmes de connectique en pratique.

Enfin, la clé privée peut se trouver sur un serveur externe.

1.2.3 Autres éléments et acteurs

Dans l'environnement du terminal, on trouve par ailleurs un serveur applicatif : celui-ci est à l'origine du besoin de signature. C'est, par exemple, le S.I. d'un organisme auquel se connecte l'utilisateur et qui contient le document à signer.

Le cas échéant, un serveur de signature peut intervenir dans le processus. Son rôle est alors de gérer le processus de signature pour le compte du serveur applicatif.

La façon dont le terminal communique et échange des données avec le ou les différents serveurs (téléphonie, Internet/GSM, Internet/Wifi) est en-dehors du cadre de cette étude.

Acteur	Rôles et responsabilités
Porteur/signataire	Propriétaire du terminal Porteur du certificat de signature
Opérateur de téléphonie	Fournit la SIM et l'accès au réseau téléphonique
Fournisseur du terminal (constructeur)	Fournit le terminal
Fournisseur d'OS	Fournit l'OS et le socle logiciel des terminaux. Le cas échéant, peut maîtriser un *secure element*.
Fournisseur de service de signature en mobilité (MSSP)	Opère, gère et fournit le service de signature (côté serveur) Fournit l'application de signature installée sur le terminal
Autorité d'enregistrement (A.E.)	Contrôle l'identité du porteur avant émission/remise du certificat (les autres rôles de l'A.E. sortent du périmètre de la présente étude)
Autorité de certification (A.C.)	Produit le certificat Gère la révocation

2 LES USAGES METIERS

2.1 Exemples concrets

2.1.1 Signature personnelle d'un document en mobilité

Dans un contexte professionnel, un salarié accède via son terminal à un document mis à sa disposition sur un S.I., tout comme il pourrait le faire depuis un poste de travail fixe. Il prend connaissance de ce document et le signe électroniquement.

Exemples :

- signature d'un P.-V. de recette
- signature d'une note de frais
- validation d'une demande de congés

2.1.2 Contractualisation électronique en mobilité

Un client souscrit un crédit à la consommation depuis son terminal : après avoir étudié différentes offres en ligne, le client porte son choix sur l'une d'elles. Il consulte les conditions générales, complète un formulaire et signe sa demande de crédit.

Signature(s) : client et organisme de crédit

Selon les cas, le client peut être préalablement connu ou non de l'organisme.

2.1.3 Procès-verbal produit en mobilité par un agent assermenté

Un huissier établit un constat chez un particulier. Il dispose d'un certificat de signature professionnel et d'un terminal mobile. Il utilise celui-ci pour constituer les différentes pièces du dossier : prise de photos, descriptions textuelles, voire enregistrement audio ou vidéo.

Une fois le dossier complet, il le signe électroniquement et l'archive en ligne sur un serveur.

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

En environnement bancaire, depuis son espace personnel, un client établit et signe des ordres de transmission à sa banque à partir de son terminal mobile. Il peut s'agir, par exemple, de paiements SEPA ou EBICS.

2.1.5 Prise de commande

Un V.R.P. en déplacement prend des commandes durant ses visites chez des prospects ou des clients (rendez-vous commerciaux). À cette occasion, il saisit des bons de commande sur son terminal mobile et les fait signer par les clients. La signature du client sert à éviter toute contestation lors de la livraison des produits, celle-ci étant préalable au paiement.

Le V.R.P. signe aussi chaque bon de commande : cette signature vise à assurer une meilleure traçabilité des prises de commande.

Signature(s) : client (acheteur) et V.R.P.

Le bon de commande peut, éventuellement, faire office de facture dématérialisée fiscalement.

2.1.6 Plan de prévention et d'intervention technique

Un technicien intervenant sur site ou dans un atelier établit et signe un compte-rendu d'exécution, dans un domaine exigeant la traçabilité et l'imputabilité des actions (ex. : aéronautique ou nucléaire, réseau gazier, etc.). Il dispose pour cela d'un terminal mobile lui donnant accès au plan d'intervention (description des actions à mener), avec lequel il remplit et signe son compte-rendu.

Signature(s) : technicien

2.1.7 Attestation de conformité

Un auditeur métier contrôle et établit des attestations de conformité d'installations, services, etc. chez ses clients. Le terminal permet de remplir le « rapport de visite » et, le cas échéant, d'établir immédiatement l'attestation de conformité.

Signature(s) : Les deux documents (rapport, attestation de conformité) sont signés par l'auditeur et seront transmis au client par e-mail.

2.2 Actions nécessaires à la signature en mobilité

Tous les exemples précédents ont en commun un processus de signature, dont la présente section détaille les étapes nécessaires.

Les actions ci-dessous sont nécessaires à la mise en œuvre de la signature électronique en mobilité, mais **leur chronologie peut toutefois varier d'un cas d'usage à un autre, et en fonction des cas métier se présentant** :

1. Enregistrement du porteur

   Au sens de l'A.E. : identifier le porteur préalablement à la délivrance du certificat de signature.

2. Création/délivrance/acceptation du certificat

   L'acceptation n'est pas nécessaire en signature simple.

3. Blocage/déblocage du PIN/signature, mécanisme de révocation

   Les utilisateurs ont tendance à perdre ou bloquer leur code PIN, lorsqu'il y en a un. La gestion post-émission du certificat peut être complexe (ou être inexistante, dans le cas d'un certificat éphémère) et est à considérer dans le choix d'une solution. Les possibilités restent néanmoins dépendantes des capacités de la puce utilisée, lesquelles peuvent être limitées pour des raisons de sécurité (matériel certifié).

Par qui et comment sont gérées ces opérations ? est un point d'attention important, car ces questions sont au centre de l'expérience utilisateur et peuvent être à l'origine du succès ou du rejet de la solution.

Remarquons qu'une façon de faire consiste à ne pas les gérer, en s'appuyant sur des certificats éphémères.

4. Visualisation des données à signer

   C'est un besoin règlementaire de la signature électronique, en mobilité ou non. Cette présentation doit permettre à l'utilisateur de comprendre ce qu'il s'apprête à signer.

5. Accord du porteur

   Autre nécessité règlementaire de la signature électronique. Le porteur doit manifester, par une action spécifique, son accord pour la signature.

6. Authentification du porteur pour la signature

   L'authentification du porteur peut s'appuyer sur un dispositif de sécurité spécifique à la signature (p. ex. code PIN d'activation de la clé privée) ou bien sur un mécanisme provenant de l'environnement (p. ex. carte SIM, verrouillage du téléphone).

   L'authentification est une conséquence de l'accord du porteur et ne peut en aucun cas le remplacer.

7. Création de la signature

La création de la signature est suivie d'une série d'opérations backoffice (cf. Document pédagogique sur la signature électronique du Club).

3 LA SIGNATURE EN MOBILITE ET LES NIVEAUX DE SIGNATURE

Rappel : Le cadre réglementaire est, à la date de rédaction du présent document, en cours de refonte dans le cadre d'un règlement européen venant réviser les textes en vigueur sur la signature électronique.

3.1 Signature simple

Selon la directive européenne (1999/93/CE) : il s'agit d'*« une donnée sous forme électronique qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification. »*

Selon l'article 1316-4 du *Code civil*, *« [La signature électronique] consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. »*

Ces textes ne posent pas 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 ; risque lié au « vol » ou à la duplication des données d'authentification.

Remarquons que la simple identification du porteur via l'IMEI (*International Mobile Equipment Identity*) ou IMSI (*International Mobile Subscriber Identity*) ne saurait suffire, pas plus qu'un numéro de « client » ou « souscripteur ». En effet, la fiabilité du procédé d'identification requise par le *Code civil* ne peut se limiter à la possession d'un équipement (en l'occurrence, le terminal lui-même ou la carte SIM qu'il contient), lequel peut être perdu, volé ou prêté. L'état de l'art répond à cette exigence via la délivrance d'un certificat électronique de signature, lequel porte l'identité de la personne à laquelle il est remis (« porteur » du certificat).

En revanche, la création du « lien logique » entre l'acte et une identité n'est pas un problème : les mécanismes d'empreinte et de signature cryptographiques répondent parfaitement à ce besoin.

3.2 Signature avancée ou sécurisée

La directive européenne parle de signature « avancée », le décret 2001-272, de signature « sécurisée ».

Selon la directive européenne (1999/93/CE), c'est *« une signature électronique qui [est] liée uniquement au signataire, [permet] d'identifier le signataire, [est] créée par des moyens que le signataire puisse garder sous son contrôle exclusif, [et] liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable. »*

Selon le décret sus-cité, *« une signature électronique qui [est] propre au signataire, […] créée par des moyens que le signataire puisse garder sous son contrôle exclusif, [et qui] garantit avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable ».*

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 (voir chapitre 5).

Ce niveau de signature est l'état de l'art de la signature électronique.

3.3 Signature qualifiée ou présumée fiable

La signature qualifiée est une notion induite par la directive européenne : *« signature électronique avancée basée sur un certificat qualifié et créée par un dispositif sécurisé de création de signature »*. Les termes « certificat qualifié » et « dispositif sécurisé de création de signature » y sont définis mais pas repris ici.

Le décret 2001-272 suit la même logique *(« une signature électronique sécurisée, établie grâce à un dispositif sécurisé de création de signature électronique et […] un certificat électronique qualifié. »*) mais, en référence à la présomption de fiabilité d'une telle signature introduite dans le *Code civil*, on parle de « signature présumée fiable ».

Ce niveau impose de fortes contraintes techniques sur le dispositif de création de signature. À ce jour, par exemple, il n'existe pas de carte SIM pouvant prétendre au titre de « *dispositif sécurisé de création de signature électronique* ».

Par ailleurs, l'immense majorité des cas d'usage ne nécessite pas l'usage de ce niveau de signature. En pratique, ce niveau est réservé à des professions particulières (officiers d'état civil, notaires, etc.).

4 LES PROBLEMATIQUES PROPRES A LA SIGNATURE EN MOBILITE

4.1 Les problématiques organisationnelles

4.1.1 L'identification du signataire

Comme expliqué ci-dessus, le signataire est identifié, dans la 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 mobile pour ce qui se rapporte au cycle de vie des certificats.

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

Si un téléphone mobile reste majoritairement personnel, une tablette l'est beaucoup moins (cadre familial) ; d'où la nécessité d'une authentification supplémentaire du signataire au moment où l'on crée la signature (le « *what you own* » peut ne pas être suffisant). Les deux méthodes les plus couramment utilisées sont :

- Le recours à un code PIN spécifique ou un mot de passe protégeant la clé de signature
- Le recours à une authentification via un canal tiers (SMS, biométrie, par exemple).

4.2 Les problématiques techniques

Nous présentons ici les contraintes liées aux ressources limitées des terminaux.

4.2.1 Visualisation des informations signées

La signature manifestant le consentement du signataire, il est nécessaire que celui-ci puisse prendre connaissance de ce qu'il va signer. 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.

Le second facteur est celui du format du document : tout dépend des capacités d'affichage du terminal (taille de l'écran, résolution, couleurs), voire des logiciels installés ou devant l'être. Signer un document PDF nécessite que le terminal dispose d'un logiciel capable de lire ce format ; idem. Pour les formats bureautique (Word, Excel).

Enfin, il existe un risque lié à l'environnement mobile lui-même : 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[2]. La question se pose aussi en ce qui concerne la confidentialité des données (code PIN, mot de passe) saisies sur le terminal.

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

Dans le même ordre d'idée que la visualisation des documents, il faut distinguer, dans une signature électronique, la signature cryptographique (simple calcul mathématique) de son formatage (création des données de signature). En effet, la mise en forme d'une signature électronique est une opération potentiellement gourmande en ressources, surtout pour les signatures dites avancées (AdES), lesquelles pouvant demander de télécharger et traiter des données tierces (jetons d'horodatage, listes de révocation).

Là encore, les ressources limitées d'un terminal peuvent être un obstacle à certains choix techniques.

4.2.3 La maîtrise de l'environnement logiciel et matériel

Ce point concerne le fournisseur d'application : les OS mobiles ont un cycle de vie court, de même que les matériels. Si l'architecture retenue s'appuie de plus sur un composant matériel tiers (carte à puce, carte SIM ou micro-SIM, clé USB), la chaîne de compatibilité s'allonge et, avec elle, le risque que la solution ne fonctionne pas.

Le point est particulièrement bloquant si un niveau de certification est visé. En effet, les schémas d'évaluation actuels ne sont pas adaptés à ce cadre dans la mesure où une certification ne concerne qu'un environnement précis (version de l'OS, type de carte à puce, modèle de terminal, etc.).

Sauf dans le cas d'une flotte de terminaux maîtrisés, la sécurité d'une plate-forme mobile sur laquelle l'utilisateur peut et est incité à installer des applications tierces reste difficile à assurer.

[2] Il n'existe pas non plus de véritable exemple de logiciel malicieux qui soit venu induire en erreur un utilisateur en modifiant les données affichées par un autre programme.

5 DIFFERENTS SCENARIOS DE SIGNATURE EN MOBILITE

5.1 Signature sur le mobile

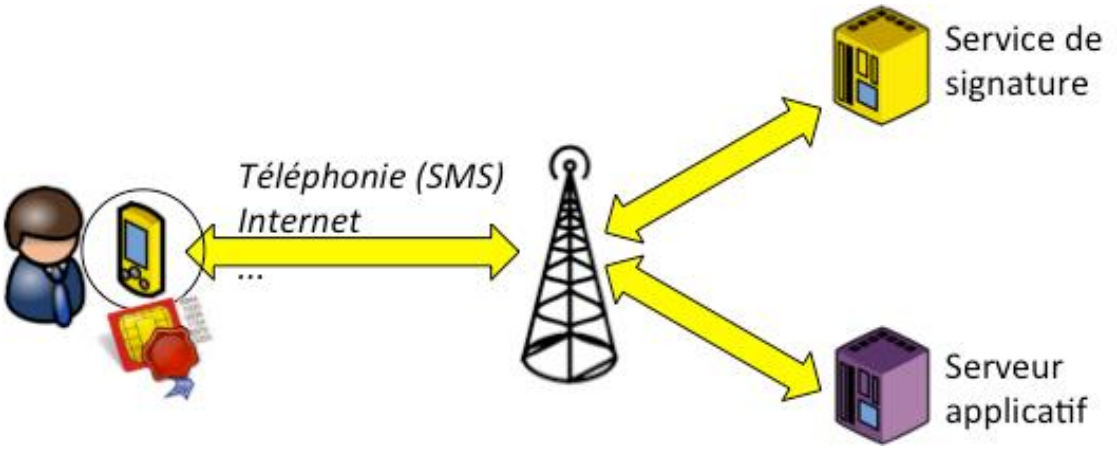
Pour effectuer une signature depuis un terminal, il n'existe que deux grandes options : soit le terminal ne sert que de moyen d'authentification du signataire, et la signature est réalisée sur un serveur qui détient la clé privée et le certificat associé, soit le terminal embarque ces éléments et réalise lui-même la signature.

Dans ce dernier cas, afin de remédier aux limitations techniques évoquées précédemment, le terminal ne réalisera en général que la signature cryptographique. Celle-ci est transmise au serveur, lequel la formate.

Quelle que soit la solution adoptée, la question de l'affichage du document à signer demeure.

5.1.1 Certificat stocké sur la SIM

Dans la mesure où la carte SIM est la propriété de l'opérateur de téléphonie, stocker les bi-clés de signature sur la carte SIM signifie soit que l'opérateur joue le rôle d'A.C., soit qu'il donne à l'A.C. un accès à « sa » carte.



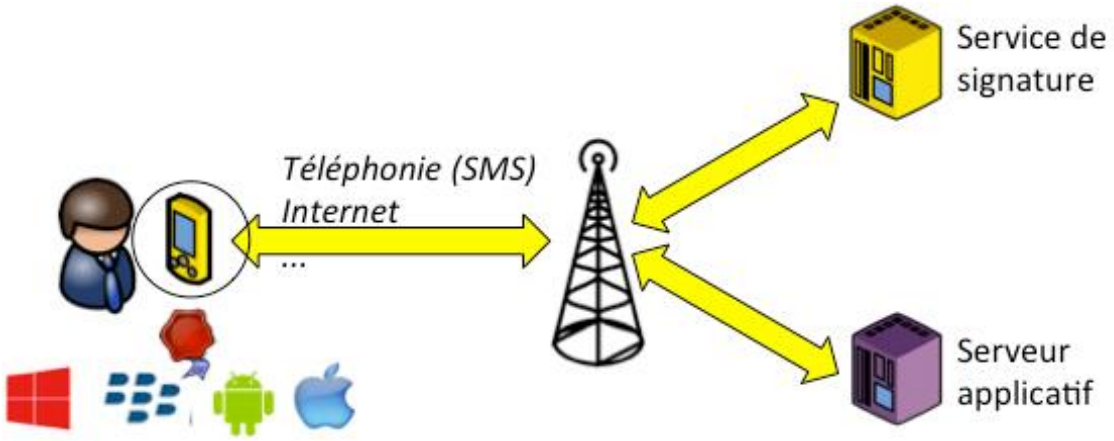
Rappelons que certains terminaux disposent de deux emplacements pour accueillir des cartes SIM. Ce type de terminal permet de séparer l'opérateur de téléphonie et l'A.C.

Avantages	Inconvénients
• Respect réglementaire : contrôle physique du porteur sur sa bi-clé • Possibilité d'avoir un code PIN propre à la signature	• Difficultés techniques : accéder à la SIM pour signer, installer le certificat, etc. • Problème organisationnel si l'opérateur de téléphonie doit intervenir dans la délivrance du certificat.

Signature simple	Signature avancée	Signature qualifiée
Oui	Oui	Non car à ce jour, aucune carte SIM certifiée SSCD ne permet de le faire

Étape	Avantages	Inconvénients
Enregistrement du porteur	Par l'opérateur ?	
Création/délivrance/acceptation du certificat	Par l'opérateur ?	Formation, suivi/audition des points de vente
Création de la signature	Par l'opérateur, en point de vente (le porteur est habitué à ce type de démarche)	
Blocage/déblocage du PIN/signature, mécanisme de révocation		
Visualisation des données à signer		
Accord du porteur	Par la SIM (contrôle du code PIN de signature)	
Authentification du porteur pour la signature	Clé privée sur un support physique	

5.1.2 Certificat stocké dans l'OS du mobile

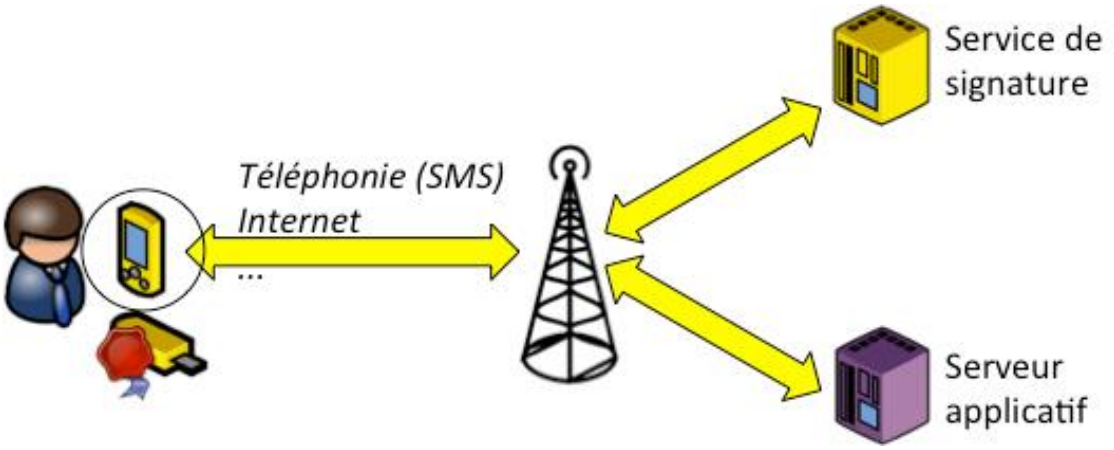


Avantages	Inconvénients
• Respect réglementaire : contrôle physique du porteur sur sa bi-clé	• Certificat logiciel (mobile « *jailbroken* » ?) • Pb organisationnel : qui gère ce certificat ? Comment le protéger ?

Signature simple	Signature avancée	Signature qualifiée
Oui	Oui	Non

Étape	Avantages	Inconvénients
Enregistrement du porteur	Sans adhérence avec l'opérateur de téléphonie	
Création/délivrance/acceptation du certificat	Sans adhérence avec l'opérateur de téléphonie	
Création de la signature		
Blocage/déblocage du PIN/signature, mécanisme de révocation		
Visualisation des données à signer		
Accord du porteur		
Authentification du porteur pour la signature	Clé privée sous le contrôle physique du porteur	Risque sur la clé privée : elle est potentiellement duplicable

5.1.3 Certificat stocké sur un *token* cryptographique (micro SD, clé USB, carte à puce)



Avantages	Inconvénients
• Respect réglementaire : contrôle physique du porteur sur sa bi-clé • Indépendance du certificat avec le terminal (A.C. totalement indépendante de la téléphonie) • Offre « standard » disponible sur le marché • Possibilité de faire de la signature qualifiée	• Difficultés techniques : accéder au *token* pour signer, transmission du code PIN (risque d'interception sur le terminal ?)

Signature simple	Signature avancée	Signature qualifiée
Oui	Oui	Oui

Étape	Avantages	Inconvénients
Enregistrement du porteur		
Création/délivrance/acceptation du certificat	Faisable par une A.C. tierce	
Création de la signature	Faisable par une A.C. tierce	Difficulté technique à intervenir sur la carte via le terminal (établissement d'un *secure channel* pour la gestion de la carte)
Blocage/déblocage du PIN/signature, mécanisme de révocation		
Visualisation des données à signer		
Accord du porteur	Par le *token*	Transmission du PIN saisi sur le terminal (mobile « *jailbroken* » ?)
Authentification du porteur pour la signature	Clé privée sur un support physique	

5.1.4 Certificat stocké dans les « *secure elements* »

Un *secure element* est, peu ou prou, un *token* durci, le plus souvent, certifié selon les Critères Communs[3]. Il peut être intégré au terminal ou être amovible. Ce cas est donc, en termes d'avantages et d'inconvénients, similaire au 5.1.3, mais sans la possibilité de faire

[3] www.commoncriteria.org

de la signature qualifiée (l'existence de « *secure element* » certifié SSCD n'est pas garantie). A ce jour, il n'existe pas de "secure element" certifié SSCD.

La SIM est considérée, dans la littérature, comme un *secure element*.

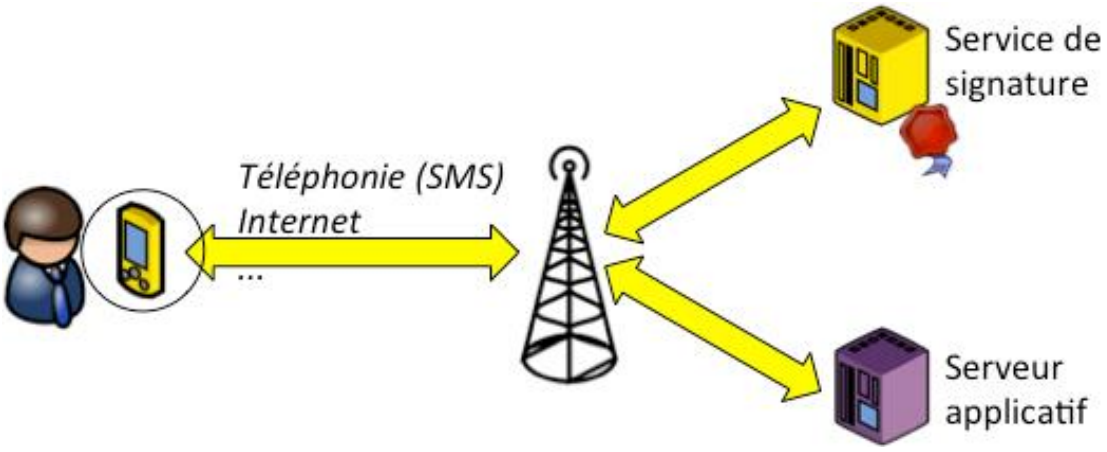
5.1.5 Autres possibilités

Issus en partie du monde bancaire et industriel (*Trusted Computing Group*), plusieurs initiatives proposent des approches alternatives pour répondre au besoin de sécurité sur un terminal mobile ou, de façon plus générale, sur tout équipement informatique. Initialement conçu comme un moyen d'assurer l'intégrité du système d'exploitation au démarrage, le *Trusted Platform Module* (TPM) est un microcontrôleur pouvant conserver des clés privées ou secrètes, des mots de passe ou des certificats, ainsi que l'implémentation des algorithmes cryptographiques associés. Il pourrait donc, en théorie, permettre d'héberger une clé privée de signature.

Le TPM étant contrôlé par le constructeur du terminal au même titre que la carte SIM l'est par l'opérateur de téléphonie, il est probable que cette solution pose, en pratique, les mêmes difficultés de gestion du cycle de vie des certificats de signature qu'en 5.1.1.

Une autre piste, celle proposée par le *Trusted Execution Environment* (TEE) de *GlobalPlatform*, imagine l'existence d'un environnement d'exécution sécurisé sur le terminal, mais indépendant de l'OS[4]. Cette solution se situe à mi-chemin entre l'utilisation d'un *secure element* (5.1.4) et le stockage du certificat par l'OS (5.1.2) ; selon ses promoteurs, elle combinerait les avantages des deux solutions (sécurité et souplesse d'utilisation). Il n'existe toutefois pas, à notre connaissance, d'application déployée de cette technologie dans le domaine de la signature électronique.

5.2 Signature déclenchée à partir du mobile



[4] http://www.globalplatform.org/documents/GlobalPlatform_TEE_White_Paper_Feb2011.pdf

Cette approche a comme principal intérêt de répondre aux questions de stockage et de protection de la clé privée des signataires : la clé privée ne réside pas sur le terminal mobile, mais sur un serveur, éventuellement doté d'un boîtier cryptographique.

On déplace ainsi ces questions sur l'authentification du signataire et les mécanismes de déclenchement de la signature. Plusieurs solutions (liste non exhaustive) sont possibles :

- saisie et transmission d'un code PIN au serveur : le code PIN protège la clé sur le serveur.
- authentification par OTP (sur le même terminal ou sur un autre) : le serveur s'assure de l'accord du porteur selon un mécanisme similaire à celui de certains schémas de paiement bancaires (3-D Secure).
- signature asynchrone : envoi d'un e-mail de confirmation contenant un lien de validation (cas limite, peu souhaitable si on s'intéresse au taux de concrétisation d'un processus de souscription ; risque de problèmes de reprise)
- double authentification : connexion sur un portail (SSL, authentification client sur la base d'un certificat pouvant être stocké dans l'un des endroits précédemment mentionnés pour le certificat de signature) et saisie du code PIN sur celui-ci.
- authentification simple : comme ci-dessus, mais sans code PIN, ce qui revient à considérer le terminal comme un *token* d'authentification.

Avantages	Inconvénients
• Indépendance du certificat avec le terminal (A.C. totalement indépendante de la téléphonie) • Offre « standard » disponible sur le marché	• « contrôle exclusif » contestable

Signature simple	Signature avancée	Signature qualifiée
Oui	Oui	Non

Étape	Avantages	Inconvénients
Enregistrement du porteur		
Création/délivrance/acceptation du certificat	Faisable par une A.C. tierce	
Création de la signature	Sur le serveur : affranchissement complet des limitations du terminal	
Blocage/déblocage du PIN/signature, mécanisme de révocation		
Visualisation des données à signer		Démontrer l'adéquation entre les données serveur et les données présentées sur le terminal
Accord du porteur		« contrôle exclusif » contestable
Authentification du porteur pour la signature	Souplesse dans le choix de la mise en œuvre	

5.3 Signature électronique à distance

Bien qu'il n'y ait pas de définition réglementaire d'une telle signature, la future norme *CEN Server signing TS 419 241* (en cours d'élaboration) et le groupe de travail *419 241 CloudSigning ETSI Workshop* travaillent sur la question, côté serveur du moins.

Le modèle, inspiré des services d'horodatage et de cachet serveur, est le suivant :

- les clés privées de signature sont hébergées dans un module cryptographique, connecté à un serveur
- ce serveur propose un « service de signature » à distance aux utilisateurs et se charge (partiellement ou totalement) du contrôle d'accès à ce service

Selon les cas, une même clé de signature peut être partagée par plusieurs utilisateurs ou être propre à chacun (cloisonnement des clés).

Dans le cadre de la directive européenne, le forum FESA *(Forum of European Supervisory Authorities for Electronic Signatures)* a envisagé, dès le début des années 2000, la possibilité de créer des signatures qualifiées depuis « un serveur » *(Public Statement on Server Based Signature Services, October 17, 2005)*.

Plus récemment, une étude présente une solution permettant de créer des signatures « répondant aux exigences d'une signature qualifiée » depuis un téléphone mobile[5]. Un fichier PDF sur le mobile (format spécifique, PDF-AS, défini pour les usages gouvernementaux[6]) est signé sur un serveur, suite à l'authentification de l'utilisateur par mot de passe, puis par OTP-SMS (appelé TAN, « *transaction number* »), soit deux facteurs par deux canaux distincts[7].

De son côté, l'Italie dispose déjà de solutions de signature qualifiées par l'autorité nationale, mais l'Allemagne l'interdit.

Cette approche semble être celle de la future norme *CEN Server signing TS 419 241,* qui identifierait deux niveaux de conformité :

- authentification par l'environnement *(level 1)*
- authentification par le dispositif de création de signature et par l'environnement (deux facteurs requis, *level 2*). Ce second niveau vise l'équivalence avec un SSCD.

Dans tous les cas, le terminal mobile joue le rôle de moyen d'authentification du signataire ; selon les cas, il participe ou non au contrôle d'accès à sa clé privée, car c'est bien là le

[5] *Qualified PDF signatures on mobile phones*, Thomas Zefferer, Arne Tauber, Bernd Zwattendorfer, Klaus Stranacher. *Electronic Government and Electronic Participation - Joint Proceedings of Ongoing Research and Projects of IFIP EGOV and IFIP ePart*, 2012, pp. 115-123.
[6] https://joinup.ec.europa.eu/software/pdf-as/description
[7] Remarque : cet OTP-SMS est intercepté par un agent sur le mobile et directement transmis à l'application de signature, sans intervention de l'utilisateur. Le TAN est envoyé/transmis au serveur de signature après que l'utilisateur a cliqué sur le bouton « signer ».

cœur des interrogations : comment assurer le « contrôle exclusif » du signataire sur ses « données de création de signature » ?

Remarquons toutefois que ce modèle n'a rien de spécifique à la mobilité du signataire, puisqu'il se concentre avant tout sur la partie serveur.

6 LES ENJEUX DU DEPLOIEMENT ET DE LA GESTION DU CYCLE DE VIE DES CERTIFICATS

Le contexte de la signature en mobilité n'apporte guère de particularité aux problèmes de gestion des certificats. Les difficultés liées à l'enrôlement, la délivrance et la révocation des certificats ne sont affectées par la présence d'un terminal que sur quelques points.

Parmi les possibilités précédemment évoquées (certificat sur la SIM, sur un serveur externe, logiciel, etc.), le premier point qui mérite attention est le risque de conflit d'autorité entre un acteur du monde mobile et l'A.C. Par exemple, le premier cas auquel on pense, c'est celui où le certificat doit être installé (par l'A.C.) sur la SIM, laquelle est sous le contrôle de l'opérateur de téléphonie.

Pareillement, l'accès à des espaces de stockage (certificat logiciel) ou des périphériques (*secure element*, support externe) peut demander des droits réservés au seul fournisseur de l'OS (droits "*root*") et constituer un obstacle technique difficilement surmontable.

Le second point est le contrôle ou non de la flotte de terminaux.

6.1 Déploiement en environnement maitrisé

On entend par environnement maîtrisé le cas d'une flotte de terminaux émis et contrôlés par un acteur unique (par exemple, une société équipant ses collaborateurs de *smartphones*). La remise du terminal à son titulaire peut, à cette occasion, s'accompagner de la délivrance du certificat.

Dans l'idéal, les terminaux sont de plus verrouillés pour empêcher toute modification (téléchargement et désinstallation d'applications, modification de la configuration, etc.) par l'utilisateur. La maîtrise du matériel et du socle logiciel permet dans ce cas d'envisager sereinement la mise en œuvre de la signature en mobilité.

6.2 Déploiement en environnement non maitrisé

La situation opposée est celle où la flotte des terminaux n'est pas contrôlée, ni contrôlable, le plus souvent, parce que les signataires sont des clients, des personnes venant avec leur propre matériel. Cette situation est de loin la plus complexe à gérer, de part la multiplicité des environnements auxquels l'application de signature sera confrontée. Dans ces conditions, la délivrance et la gestion d'un certificat sur le terminal est, en l'état actuel de la technologie, quasiment inenvisageable.

7 LES REGLEMENTATIONS

7.1 Actuelles

7.1.1 Française

- Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique (J.O. du 14 mars 2000, p. 3968)
- Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (J.O. du 22 juin 2004, p. 11168 et s.)
- Ordonnance n° 2005-674 du 16 juin 2005 relative à l'accomplissement de certaines formalités contractuelles par voie électronique (J.O. du 17 juin 2005, p. 10342)
- Décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du *Code civil* et relatif à la signature électronique (J.O. du 31 mars 2001, p. 5070)

7.1.2 Européenne

- Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques (J.O.C.E., n° L.013 du 19 janvier 2000, p. 12 et s.)

7.2 À venir

La Commission européenne a rendu public en 2012 un projet de règlement créant un cadre européen pour l'identification électronique. Ce projet vise à remplacer et à compléter la directive européenne 1999/93/CE. En France, ce projet remplacera la loi n° 2000-230 sur la signature électronique, qui transposait cette directive.

Le règlement introduit la notion d'identité numérique et le cadre de sa reconnaissance entre États membres.

8 LES NORMES

8.1 ETSI TR 102 203 V1.1.1 (2003-05)

Présente les exigences *fonctionnelles* pour un « service de signature en mobilité ». Les exigences de sécurité sont décrites dans le document *TS 102 206 – Security Requirements for Mobile Signature Systems.*

Cette norme a pour origine la constatation que nombre de personnes disposent d'un équipement nomade contenant une carte à puce et un lecteur de carte à puce : leur téléphone, et que la possession d'un tel matériel est nécessaire pour la création d'une signature électronique de qualité.

Signature en mobilité : « moyen universel permettant à un citoyen d'utiliser un équipement nomade *[mobile device]* pour approuver une transaction ».

Équipement nomade : « tout équipement s'appuyant sur un réseau de téléphonie *[mobile network]*, avec ou sans carte à puce ». L'équipement est considéré comme l'outil de signature électronique, au même titre que le stylo pour la signature manuscrite.

N'exclut pas la cryptographie symétrique

8.2 CEN TS 419 241

Cette norme est en cours d'élaboration (fin 2013) et concerne plus directement la signature sur serveur (à distance) que la précédente.

Cette norme définit deux niveaux de conformité :

- authentification par l'environnement *(level 1)*
- authentification par le dispositif de création de signature et par l'environnement (deux facteurs requis, *level 2*). Ce second niveau vise l'équivalence avec un SSCD.

Dans tous les cas, le terminal mobile joue le rôle de moyen d'authentification du signataire ; selon les cas, il participe ou non au contrôle d'accès à sa clé privée.

8.3 ETSI Mobile Commerce (M-COMM)

- *Mobile Signatures Business and Functional Requirements, ETSI TR 102 203 V1.1.1 (2003-05)*
- *Mobile Signature Web Service Interfaces, ETSI TS 102 204*
- *Security Requirements for Mobile Signature Systems, ETSI TS 102 206*
- *Roaming of Mobile Signature Service Transactions, ETSI TS 102 207*

8.4 En cours d'élaboration

- *Architecture for Advanced AdES in distributed environments, ETSI TS 119 152*
- ETSI SR 019 020 v.0.0.0.4 pose les bases d'une future norme ETSI pour la signature en mobilité.