ROYAUME DU MAROC

OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE
---

(19)

المملكة المغربية

المكتب المغربي للملكية الصناعية و التجارية
---

(12) FASCICULE DE BREVET

(11) N° de publication :
MA 34114 B1

(43) Date de publication :
03.04.2013

(51) Cl. internationale :
H04W 12/00; H04L 9/00; G06F 00/00

(21) N° Dépôt :
34116

(22) Date de Dépôt :
24.08.2011

(71) Demandeur(s) :
ISECURE, AGDAL 6 RUE DAYET AOUA 4EME ETAGE APP 16 RABAT (MA)

(72) Inventeur(s) :
EL HOUSSAIN BENMESSAOUD

(74) Mandataire :
EL HOUSSAIN BENMESSAOUD

(54) Titre : **SYSTEME DE SIGNATURE ELECTRONIQUE EN LIGNE DE DOCUMENTS (MODE SAAS)**

(57) Abrégé : LA PRESENTE INVENTION CONCERNE UN SYSTÈME DE SIGNATURE ELECTRONIQUE DE DOCUMENTS ELECTRONIQUE. CE SYSTÈME EST CARACTÉRISÉ PAR: -NON NÉCESSITÉ D'INSTALLER UN LOGICIEL DE SIGNATURE SUR LE POSTE DE L'UTILISATEUR -LE DOCUMENT À SIGNER N'EST PAS ENVOYÉ AU SERVEUR -ACCESSIBILITÉ À DISTANCE À TRAVERS TOUS LES TERMINAUX ÉQUIPÉS D'UN NAVIGATEUR WEB (PC, MOBILE...)

Abrégé

La présente invention concerne un Système de signature électronique en ligne de documents électronique.

Ce système est caractérisé par :

- **Non nécessité d'installer un logiciel de signature sur le poste de l'utilisateur.**
- **Le document à signer n'est pas envoyé au serveur.**
- **Accessibilité à distance à travers tous les terminaux équipés d'un navigateur web (PC, mobile...)**

Description

Introduction

La dématérialisation des données existe depuis un certain temps déjà : beaucoup d'entreprises ou d'organismes, beaucoup de particuliers aussi travaillent sur des documents électroniques, les échangent, les stockent. Mais lorsqu'il s'agit de documents contractuels (contrats, factures, avenants..) ou sensibles, ces données sont imprimées pour être envoyées par courrier papier signé.

L'objet de la dématérialisation est de transformer ou conserver sous format électronique les données échangées dans le cadre d'activités professionnelles ou privées, dans les conditions légales qui permettent de conserver les mêmes garanties qu'un échange ou stockage papier. Son développement est résolument engagé : la dématérialisation apporte des avantages indéniables en termes de réduction de coûts administratifs, de gains de temps, ainsi que dans l'amélioration des processus métier.

La signature électronique est -dans bien des cas- la pierre angulaire nécessaire au déploiement de ces projets

Le présent document constitue un descriptif fonctionnel et technique de la solution de signature électronique en mode hébergée Web ou SaaS (pour Software As A Service) que nous souhaitons breveter.

Domaine technique de l'invention

Notre invention est une combinaison modifiée et adaptée de deux domaines informatiques : **La signature électronique** et le **modèle SaaS (Software As A Service)**

La signature électronique

La signature numérique est un mécanisme permettant de garantir l'intégrité d'un document électronique et d'en authentifier l'auteur, par analogie avec la signature manuscrite d'un document papier. Un mécanisme de signature numérique doit présenter les propriétés suivantes :

- Il doit permettre au lecteur d'un document d'identifier la personne ou l'organisme qui a apposé sa signature.
- Il doit garantir que le document n'a pas été altéré entre l'instant où l'auteur l'a signé et le moment où le lecteur le consulte.

Pour cela, les conditions suivantes doivent être réunies :

- Authentique : L'identité du signataire doit pouvoir être retrouvée de manière certaine.
- Infalsifiable : La signature ne peut pas être falsifiée. Quelqu'un ne peut se faire passer pour un autre.
- Non réutilisable: La signature n'est pas réutilisable. Elle fait partie du document signé et ne peut être déplacée sur un autre document.
- Inaltérable : Un document signé est inaltérable. Une fois qu'il est signé, on ne peut plus le modifier.
- Irrévocable : La personne qui a signé ne peut le nier

Le modèle SaaS

Le logiciel en tant que service ou en anglais le Software as a Service (SaaS) est un concept consistant à proposer un abonnement à un logiciel plutôt que l'achat d'une licence. Avec le développement des Technologies de l'information et de la communication, de plus en plus d'offres SaaS se font au travers du web. Il n'y a alors plus besoin d'installer une application de bureau , mais d'utiliser un programme client-serveur. Ce concept, apparu au début des années 2000, prend la suite de celui du fournisseur de service d'application (« application service provider » - ASP).

SaaS est un modèle de livraison de solution où l'éditeur/constructeur fournit des moyens et où le fournisseur de service propose (généralement dans le cadre d'un abonnement récurrent) la fonctionnalité intégrée et gérée à ses clients qui l'utiliseront. Les clients ne paient pas pour posséder le logiciel en lui-même mais plutôt pour l'utiliser.

Les principales applications actuelles de ce modèle sont le gestionnaire de relation client (CRM), la vidéo conférence, la gestion des ressources humaines, les communications unifiées, le travail collaboratif, les courriels...

SaaS est donc la livraison conjointe de moyens, de services et d'expertise qui permettent aux entreprises d'externaliser intégralement un aspect de leur système d'information (messagerie, sécurité...) et de l'assimiler à un coût de fonctionnement plutôt qu'à un investissement.

Etat de la technique antérieure

Jusqu'à présent les procédés de signature électronique utilisant les systèmes PKI (Public Key Infrastructure) nécessitent :

- **L'installation d'un logiciel de signature sur le poste local du signataire**
- **L'envoie du fichier à signer vers le serveur de signature en cas d'une signature à distance (à travers Internet)**

Description du procédé

Titre de l'invention : **Système de signature électronique en ligne de documents (Mode SaaS)**

Au contraire des deux limitations indiquées dans le chapitre (Etat de la technique antérieure). La présente invention ne nécessite pas :

- **L'installation d'un logiciel de signature électronique sur le poste du signataire**
- **L'envoie du fichier à signer vers le serveur. Le document à signer est et restera sur le poste local du signataire**

Description fonctionnelle

Grace à la loi 53-05, la juridiction marocaine offre l'équivalence juridique entre les documents établis sur support papier et ceux sur support électronique à condition qu'il soit signé électroniquement.

Notre invention permettra d'offrir la possibilité de signer électroniquement les documents électroniques sans avoir à installer un logiciel de signature sur le poste du signataire. Une simple connexion internet et un dispositif (PC ou mobile) doté de navigateur sont suffisants pour se connecter à notre serveur à distance et signer les documents en ligne à travers internet.

Une deuxième particularité de notre procédé est qu'il n'est pas nécessaire d'envoyer le document à signer vers notre serveur. Tout se passe sur le poste du signataire. Notre procédé consiste justement à envoyer tout les éléments techniques ainsi que le module de signature pour s'exécuter directement sur le poste du client de façon complètement transparente.

Description technique

Pré-requis

Le procédé nécessite pour fonctionner un certain nombre de pré-requis.

- Un certificat électronique X509 valide de signature électronique installé
- Connexion Internet à partir son PC ou de son mobile
- Navigateur internet (sur PC ou Mobile) récent

Exposé de la solution

L'enchainement de fonctionnement de notre système est comme suite :

Etape 1 : Un utilisateur adhérent à notre service se connecte au serveur à travers internet en HTTP ou HTTPS et choisi la fonctionnalité de signer un fichier électronique. Il est ensuite amener à choisir la qualité et le format de la signature souhaité conformément au format du fichier à signer

Etape 2 : l'utilisateur doit indiquer s'il désire signer avec un certificat matériel ou logiciel, et ce en cliquant sur le bouton approprié

Etape 3 : Le serveur envoie au client le code du module de signature pour s'executer sur le navigateur du client. Le module s'ouvre permettant à l'utilisateur d'indiquer le fichier à signer, son certificat, ainsi que quelques informations complémentaires (mot de passe du certificat, type d'engagement, lieu de signature), puis il clique sur le bouton « Signer »

Etape 4 : Le système afficher l'état de l'opération de signature, avec indication de l'emplacement du fichier signé en local sur le poste du signataire.

Le procédé objet du brevet, mettra en ouvre une signature électronique au format simple ou avancée grâce à l'utilisation d'un certificat électronique de signature au format **X509** fourni sous forme logicielle (**PKCS#12**) ou matérielle (carte à puce ou clé USB cryptographique) accessible à travers le protocole **PKCS #11**. La communication entre le client (navigateur de l'utilisateur installé sur son poste ou sur son mobile) et le serveur se fait à travers internet à l'aide des protocoles du WEB **HTTP/HTTPS** (Voir Figure 1)

Pour résumé : le fichier n'a pas été envoyé au serveur, il a été signé sur le poste du client, seules des informations concernant l'identification sont envoyées au serveur pour des raisons de comptabilité et gestion. Le document à signer est et reste sur le poste du client. Sa signature s'est effectuée sans installation d'un logiciel de signature quelconque sur le poste local.

Exposé du mode de réalisation

Nous avons réalisé une implémentation de ce système grâce à l'utilisation des **applets Java** permettant de s'exécuter à distance sur tout navigateur compatible Java.

Notre serveur a été également réalisé grâce à la technologie **J2EE (Java 2 Entreprise Edition)** pour envoyer le module de signature (Applet) vers le navigateur de l'utilisateur et commander l'opération de signature électronique à travers internet (en ligne) (Voir Figure 1)

Nos tests ont été effectué à l'aide de certificat de signature logiciel et matériel compatible au format de certificat normalisé **X.509v3.** Nous avons crée des signatures au format simple comme

CMS Advanced Electronic Signature ETSI TS 101 733 et également des signatures au format avancé comme **XAdES: XML Advanced Electronic Signature ETSI TS 101 903**

Applications industrielles

Le procédé objet du brevet permet d'offrir les avantages suivants :

- Gain en délais de transmission des documents originaux
- Réduire significativement les coûts de traitement des documents (impression, affranchissement, saisies des données du papier vers les systèmes d'information, mise à disposition...)
- Permettre de remplacer la signature manuscrite traditionnelle par une signature électronique offrant les mêmes garanties légales (dans le cas d'utilisation de certificat de signature sécurisé obtenu auprès d'Prestataire de Service de Certiication Electronique agréé) et une capacité supérieure en vérification
- Intégrer les échanges dématérialisés sécurisés (signer ou valider des signatures à destination ou en provenance de tiers), sans avoir à posséder en propre une infrastructure de confiance
- Doter vos documents électroniques d'une intégrité totale et pérenne dans le temps grâce à l'Horodatage permettant d'apposer une marque de temps de protection de toute contestation concernant la date d'émission ou de réception d'un fichier et permettant de certifier sa non altération entre la date d'horodatage et celle de vérification
- Sécuriser l'identité du signataire et permettre de vérifier à tout moment l'émetteur d'un document électronique

L'invention objet de la présente est susceptible -entre autre- d'application industrielle dans les domaines suivants :

- La gestion des ressources humaines: signature électronique du dossier salarié (bulletins de paie, demandes de congés, notes de frais);
- La gestion des factures électroniques et l'échange de facture et devis entre fournisseurs/clients;
- La signature électronique des pièces administratives et comptables; la signature électronique des feuilles de soins dans le secteur de la santé;
- Dépôts des dossiers de candidature aux appels d'offres publics dématérialisés et soumissions aux marchés publics
- Vote électronique avec accusé de réception signé

Revendications d'innovation

Les revendications portent sur :

1. **Le système de signature électronique de document en ligne (mode SAAS Software As A Service) à travers un client léger (navigateur internet) à l'aide d'une connexion HTTP ou HTTPS ou tout autre protocole WEB sans avoir à n'installer aucun logiciel de signature sur le poste local du signataire. Nous entendons par poste local un PC ou un terminal mobile.**

2. **Le procédé d'envoi des binaires du module de signature vers le poste du client à travers les protocoles du WEB (HTTP ou HTTPS entre autre) permettant ainsi l'exécution du module de signature en local et évitant l'envoi du fichier à signer vers le serveur pour une meilleure confidentialité de l'opération**

Dessin

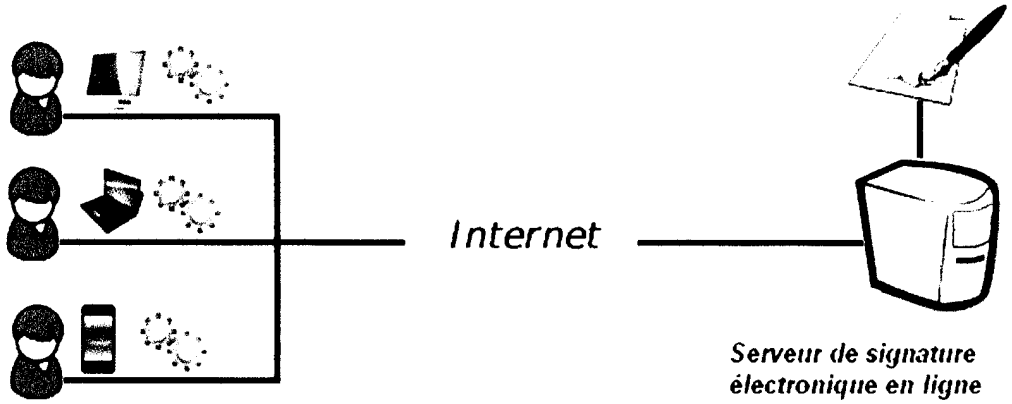

Figure 1 – système de signature électronique en ligne (en mode SaaS)