ROYAUME DU MAROC

OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE
---

(19) OMPIC

المملكة المغربية
المكتب المغربي للملكية الصناعية و التجارية

(12) BREVET D'INVENTION

(11) N° de publication :
MA 59013 B1

(43) Date de publication :
28.02.2023

(51) Cl. internationale :
G06Q 20/02; H04L 9/32; G06Q 20/38

(21) N° Dépôt :
59013

(22) Date de Dépôt :
16.07.2019

(71) Demandeur(s) :
Lleidanetworks Serveis Telemàtics, S.A., Parc Científic i Tecnològic Agroalimentari de Lleida 25003 Lleida (ES)

(72) Inventeur(s) :
SAPENA, Francisco ; SOLA, Carolina

(74) Mandataire :
M. Mehdi SALMOUNI-ZERHOUNI
(86) N° de dépôt auprès de l'organisme de validation : EP19382602.1

(54) Titre : **PROCÉDÉ DE SIGNATURE ÉLECTRONIQUE DE CONTRATS**

(57) Abrégé : L'invention concerne un procédé de signature électronique de contrats entre au moins une première et une seconde parties, le procédé comprenant une première partie accédant au site Web de la seconde partie et remplissant un formulaire en ligne avec des données personnelles de partie qui sont envoyées au serveur d'une seconde partie. Le procédé de l'invention résout le problème de la signature de contrats entre deux parties, par conséquent l'objet de la présente invention est un procédé mis en œuvre par ordinateur qui traite de la question de la protection contre l'utilisation non autorisée de données au sein des employés des sociétés TTP et nous présentons un solution dans laquelle une entreprise TTP peut certifier la validité d'un contrat sans avoir accès à son contenu. De cette manière, le TTP minimise les informations auxquelles il a accès et réduit les risques dérivés de ces connaissances, comme une éventuelle fuite de données causée par un employé malhonnête du TTP.

REVENDICATIONS

1. Méthode de signature électronique de contrats entre au moins un premier et un Deuxième partie, la méthode comprenant la première partie accédant au remplissage d'un formulaire en ligne du serveur d'une seconde partie, la méthode comprend :

a. Le serveur de la deuxième partie :

i. compiler les données personnelles fournies par la première partie, ainsi que les termes et conditions du contrat,

ii. la création d'un identifiant unique (ID),

iii. l'inclusion dudit identifiant unique (ID) dans le contrat,

iv. générer une clé aléatoire chiffrant le contrat,

v. v. chiffrer ladite clé aléatoire avec une clé publique de tiers de confiance (TTP) d'une paire de clés publiques et privées TPP, dans laquelle la clé publique est correctement certifiée et partagée et la clé privée est gardée secrète à l'intérieur du tiers de confiance (TTP),

vi. calcul d'un condensé de hachage H(ID)

vii. l'envoi du contrat chiffré, de la clé aléatoire chiffrée et du condensé de hachage H(ID) au tiers de confiance (TTP),

b. le TTP plaçant le contrat crypté dans un serveur accessible au public et l'envoi de l'URL du serveur accessible au public au serveur du second tiers,

c. le serveur de la deuxième partie envoyant l'URL du serveur accessible au public et la clé aléatoire à la première partie,

d. le téléchargement de première partie à partir du tiers de confiance (TTP), décryptage et accès à l'aide de la clé aléatoire, le contrat,

e. le tiers de confiance (TTP) recevant de la première partie l'ID à l'intérieur du contrat déchiffré et comparant un hachage dudit ID à H(ID)

reçu du serveur de la seconde partie une preuve que le contrat a été consulté par la premièrepartie lorsque les hachages correspondent,

f. lorsque les hachages correspondent, le tiers de confiance (TTP) génère et envoie un SMS ou un e-mail contenant un mot de passe à usage unique (OTP) à la première partie,

g. la première partie répondant au SMS ou à l'e-mail envoyé par un tiers de confiance (TTP) saisissant l'OTP reçu indiquant l'accord de la première partie avec le contrat,

h. le tiers de confiance (TTP) recevant et vérifiant la validité de l'OTP,

i. lors de la validation de l'OTP, le tiers de confiance (TTP) compilant tous les tinformations techniques et création d'un document de certificat qui comprend :

i. le contrat crypté,

ii. la clé aléatoire chiffrée,

iii. l'ID haché,

iv. une pièce d'identité de la première partie,

v. le numéro de téléphone ou l'adresse électronique à laquelle le BdP a été envoyé ;

vi. heure à laquelle l'OTP de confirmation a été généré.

j. horodatage du document de certificat et stockage du document de certificat horodaté sur le système d'information du tiers de confiance (TTP).

2. Procédé selon la revendication 1 dans lequel le site web est hébergé dans une IP comprise dans le domaine IP de la seconde partie.

3. Procédé selon la revendication 1 dans lequel l'OTP est transmis par numéro de téléphone ou par courrier électronique.

4. Procédé selon la revendication 1 dans lequel le tiers de confiance (TTP) est connecté au serveur de deuxième partie utilisant un VPN (Virtual Private Network).

5. Procédé selon la revendication 1 dans lequel la clé privée de la paire de clés publiques et privées de tiers de confiance (TTP) est gardée secrète par un ensemble très restreint de personnes hautement fiables à l'intérieur du TTP.