(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 1 688 891 B1**

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
31.03.2010 Bulletin 2010/13

(51) Int Cl.:
G07D 7/00 *(2006.01)*

(21) Application number: **05002155.9**

(22) Date of filing: **02.02.2005**

(54) **Electronic certification and authentication system**

Elektronische Vorrichtung zur Beglaubigung und Authentifizierung

Dispositif électronique de certification et d'authentification

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU MC NL PL PT RO SE SI SK TR
Designated Extension States:
AL BA HR LV MK YU

(43) Date of publication of application:
09.08.2006 Bulletin 2006/32

(73) Proprietor: **Geoffrey, Mohammed A.**
21434 Jeddah (SA)

(72) Inventor: **Geoffrey, Mohammed A.**
21434 Jeddah (SA)

(74) Representative: **Jehle, Volker Armin et al**
Bosch Jehle Patentanwaltsgesellschaft mbH
Flüggenstrasse 13
80639 München (DE)

(56) References cited:
US-A1- 2002 023 220

EP 1 688 891 B1

Printed by Jouve, 75001 PARIS (FR)

Description

Background of the Invention

[0001] The invention relates to electronic document security systems and in particular to the certification and authentication of document information of various type, like whole documents, certificates, signatures, stamps, etc., especially by verifying its correctness and safety / immunity from fraud.

[0002] Current systems use stickers, thermal stamps and watermarks to safeguard against and to discover fraud, mostly by using the naked eye as a detector. The naked eye poses the problem that it is relatively unreliable so that many cases of fraud occur.

[0003] There exists a need to improve certification and authentification of document information by more reliable means.

Detailed Description of Invention

[0004] The invention uses an electronic system which comprises at least the modules 1, 2, 3, 4, 7 as follows:

1. Main Module. One of the main modules tasks is it to grant access to the system on the highest level. A further task is it to create crypto-data for use with the system, such as system key pairs generated by asymmetrical crypto-algorithms. It typically runs on an application server / server system which connects to a database server / server system. The server is preferably placed in a trusted environment (e.g. as a trust centre), as for example in the data centre of certification offices. The main module updates its data by connecting to this database and/or to other databases and/or by connecting to other modules. This module is preferably used / activated by an intemet browser that runs on a PC but can also accessed by other means like programmable interfaces to other programs. The user / supervisor of this module can for e.g. create a system key pair(s), enter administrator rights and information, and enroll administrator signatures.

2. Admin Module. An administrator can use this module to, for example:

a) Enter certification office information and stamp to be stored in the system;
b) Enter certification office registrars' information and enroll their signatures;
c) Activate or deactivate certification office registrars;
d) Provide certification office registrars with user IDs and passwords;
e) Print admin reports.

The access to this module is typically granted by entering an administrator ID, password and signature into the module but can also be done in other ways, like by fingerprint sensors, ID cards etc.

3. Registration Module. A registrar can use this module to typically:

a) Enter companies' information required for certification like letter header, letter footer and stamp;
b) Register companies members' information and enroll their signatures on, e.g., a digital pad and an electronic pen connected to a PC;
c) Activate or deactivate signatories or companies' members;
d) Provide companies' members with their IDs and passwords;
e) Print member transaction reports.

The access to this module is typically granted by entering a registrar ID number, password and signature but can also be done in other ways, like by fingerprint sensors, ID cards etc.

4. Certification Module as in claim 1.
The access to this module is typically granted by entering a member ID number, password and signature but can also be done in other ways, like by fingerprint sensors, ID cards etc. Preferably, a transaction amount is directly deducted from the member account. The certified document information is preferably saved in the database.

5. Authorization Module: an authorized person can use this module esp. to print a certified letter on his printer that is connected to his PC. Preferably, all of the authorization information is saved in the database for future retrieval.

6. Online Verification Module: a verifier can use this module to esp. do the following:

a) Retrieving a document to be verified by, e.g., entering the document certification number.
b) Comparing and/or printing the information displayed to verify its correctness and safety from fraud.

The above described modules are preferably run on the application server / server system and are preferably connected to an data network like the intemet and activated by, for example, an intemet browser that runs on a PC. Thus, users from different levels can access their modules from anywhere. Preferably, the modules check the corresponding user's ID number, password and / or signature before granting access to the respective module.
Altematively or in parallel to the Online Verification

Module, the system can comprise:

7. An Offline Verification Module as in claim 1.

[0005] In order that the invention may be more readily understood and put into practical effect, a preferred embodiment of the invention will now be described with reference to the accompanying drawings, in which :

FIG.1 schematically shows a handwritten signature captured by a digital pad and an electronic pen;

FIG.2 schematically shows a company stamp,

FIG.3 schematically shows a certification office stamp,

FIG.4 schematically shows a 2D barcode.

[0006] The modules of this invention are linked to each other and preferably share one database, and work as one system.

[0007] The process to use the system usually starts with an authorized person to enter admin information (name, position, adress, IP adress, admin ID, password etc) and at least one, preferably three or more, electronic admin signatures into the Main Module.

[0008] The admin is then allowed to log into the Admin Module, e.g. by entering his user ID, password, and electronic signature; this can be done by using an internet or intranet browser and a digital pad and electronic pen, for example. The admin is thus not restricted to use a closed network and can access the admin module from anywhere.

[0009] The admin in turn can grant access to the Certification Module by entering registrar information (name, employing certification office, address, IP address, registrar ID, password etc) and at least one, preferably three or more, electronic registrar signatures. The registrar is then allowed to log into the Registration Module, e.g. by entering his user ID, password, and electronic signature; this can be done by using an intemet or intranet browser and a digital pad and electronic pen, for example. The registrar is thus not restricted to use a closed network and can access the Registration Module from anywhere.

[0010] The registrar on the other hand, who usually works for a trusted, often govemmental, organisation like a certification office, can can grant access to the Certification Module to a member of another organisation (often a commercial company) by entering the member information (name, employing company, address, IP address, member ID number, password etc) and at least one, preferably three or more, electronic member signatures. The member is then allowed to log into the Certification Module, e.g. by entering his user ID, password, and electronic signature; this can be done by using an internet or intranet browser and a digital pad and electronic pen, for example.

[0011] Members using the Certification Module can enter document information after enrolling their signature (s) into the system, e.g. on a digital pad with an electronic pen connect to a PC. After that, the system compares the enrolled signature patterns with the signatures pattern(s) stored in the database to verify the correctness of the signature. If the signature has been positively verified, the document information is stored in the database, thus completing the certification process.

[0012] A member can also use the system to print, e.g., one or more of: the member's signature, as shown in FIG. 1, his company stamp as shown in FIG.2, a certification office stamp as shown in FIG.3, a certification number, a certification date, a certification time, and a 2D barcode as shown in FIG.4. Printing can be done by using a printer connected to the member's PC or using a PC on a third person's printer wherein the third person is authorized to print the document. The authentication process is then complete.

[0013] A typical 2D barcode usually has bars placed on the horizontal and the vertical dimension (as shown schematically in Fig. 4) and is generated using a 2D barcode generation program which transfers information into bars form. To be able to encode longer documents in barcode form, the document information is compressed. In order to prevent forgery and fraud, encrypted information is added. Document information and encrypted information are both put into the 2D barcode. The 2D barcode can be generated by:

- encrypting the compressed document information with a system generated random key, encrypting the random key with a system encryption key and generating the 2D barcode from the encrypted random key and the encrypted compressed document information.

[0014] The encryption key is preferably one key out of a key pair, as for example from a asymmetric encription algorithm (e.g. PKI).

[0015] The 2D barcode can, for example, contain the following:

1. document information
2. member name
3. company name
4. certification office name
5. certification office stamp
6. system decryption key name
7. random key or hash code.

[0016] The Offline Verification Module enables verifiers to read the 2D barcode after scanning the document and to display the corresponding information.

[0017] The decryption can be carried out by:

- decrypting the random key by the system decryption key, decrypt the compressed document infor-

mation using the random key.

After that, the compressed document information is decompressed and the module displays it so that the verifier can compare this document information with the printed document information to verify the correctness and safety of the document from fraud.

[0018] The verifier can verify using the Online Verification Module through the Intemet from displaying the certified document information to verify the correctness and safety of the document from fraud.

Claims

1. A system for electronic certification and authentication, comprising the following components:

a Main Module which grants access to an Admin Module and which provides crypto-data, especially a crypto key pair comprising a system encryption key and a system decryption key, for use with the system;
- wherein the Admin Module is provided to at least:

(i) enter and store certification office information;
(ii) grant access to a Registration Module by entering and storing at least a registrar's information and registrar's at least one electronic signature;
(iii) activate or deactivate registrars;
(iv) provide registrars with user IDs and passwords;

- wherein the Registration Module is provided to at least:

(i) enter a company Information;
(ii) register a company member's information and enroll member's signatures;
(iii) activate or deactivate signatories or company members; and
(iv) provide the company member with member's ID and password;

- a Certification Module which is provided to at least:

(i) enter and save the document information intended for certification;
(ii) enroll the member's signature; and
(iii) compare the enrolled signature with the stored member's signatures, wherein if the enrolled signature matches the stored member's signatures, then said Certification Module is further to:

generate a 2D barcode by encrypting the document information using a random key; and the certification module is further to:

produce the certified document including the document information and the random key

- an Offline Verification Module that runs on a stand alone verifier data system which is provided to at least:

(i) receive the certified document;
(ii) decrypt the random key using the system decryption key;
(iii) decrypt the document information using the random key;

characterized in that the Certification Module is further to: generate the 2D barcode by encrypting the random key using the system encryption key, wherein said encrypted random key is capable of being decrypted using the system decryption key;
further **characterized in that** the Offline Verification Module is further provided to: display the information contained in the 2D barcode, the information comprising the encrypted random key.

2. The system of Claim 1, wherein the 2D barcode is generated by the following steps:

(i) compressing the document information;
(ii) encrypting the compressed document information with a system generated random key,
(iii) encrypting the random key with a system encryption key from the Main Module, and
(iv) generating the 2D barcode from the encrypted random key and the encrypted compressed document information.

3. The system of Claim 2, further comprising an Offline Verification Module which is provided to at least:

(i) scan the certified document;
(ii) decrypt the random key with the system decryption key,
(iii) decrypt the compressed document information with the random key;
(iv) decompress the document information;
(v) compare the document information from the 2D barcode with another shown document information.

4. The system of Claim 1, wherein the 2D barcode is generated by the following steps:

(i) compressing the document information;
(ii) encrypting the compressed document information Hash code with a system encryption key from the Main Module,
(iii) generating the 2D barcode from the encrypted Hash code and the compressed document information.

5. The system of Claim 4, further comprising an Offline Verification Module which is provided to at least:

(i) scan the certified document;
(ii) decrypt the random key with the system decryption key,
(iii) decrypt the hash code with the system decryption key,
(iv) compare the hash code with the compressed document information hash code;
(iv) decompress the document information;
(v) compare the document information from the 2D barcode with another shown document information.

6. The system of one of the Claims 1 to 5, wherein the signature is enrolled by the way of a digital pad and an electronic pen.

7. The system of one of the Claims 1 to 6, wherein the access to one of the modules is granted by entering an ID number, a password, and an electronic signature.

8. The system of one of the Claims 1 to 7, wherein at least one of the modules can be accessed over the internet using an internet browser.

9. The system of one of the Claims 1 to 8, wherein at least the Main Module, Admin Module, and Registration Module are run on the same application server.

10. A 2D barcode for the certification and authentication of document information, containing at least the compressed document information and a crypto key for verification and/or encryption of the document information.

Patentansprüche

1. System zur elektronischen Zertifizierung und Authentifizierung, mit den folgenden Komponenten:

- einem Hauptmodul welches Zugriff auf ein Admin Modul zulässt und Krypto-Daten bereitstellt, insbesondere ein Krypto-Schlüssel-Paar mit einem System-Verschlüsselungs-Schlüssel und einem System-Entschlüsselungs-Schlüssel zur Verwendung in dem System;
- wobei das Admin Modul bereitgestellt ist um zumindest:

(i) Zertifizier-Stellen-Information einzugeben und zu speichern;
(ii) Zugriff auf ein Registrations-Modul zuzulassen, indem zumindest Registrator-Informationen und zumindest eine elektronische Unterschrift des Registrators eingegeben und gespeichert werden;
(iii) Registratoren zu aktivieren oder deaktivieren;
(iv) Registratoren Nutzer-IDs und Passwörter bereitzustellen;

- wobei das Registrations-Modul bereitgestellt ist um zumindest:

(i) Firmen-Information einzugeben;
(ii) Firmen-Mitglieds-Informationen zu registrieren und Unterschriften von Mitgliedern zu registrieren;
(iii) Signaturen oder Firmen-Mitglieder zu aktivieren oder deaktivieren; und
(iv) für Firmen-Mitglieder Mitglied-ID und Paßwort bereitzustellen;

- ein Zertifizier-Modul, welches bereitgestellt ist um zumindest:

(i) Dokumenten-Information welche zur Zertifizierung gedacht ist einzugeben und zu speichern;
(ii) die Unterschrift von Mitgliedern zu registrieren; und
(iii) die registrierte Unterschrift mit den gespeicherten Unterschriften von Mitgliedern zu vergleichen, wobei dann, wenn die registrierte Unterschrift mit den gespeicherten Unterschriften von Mitgliedern übereinstimmt, das Zertifizier-Modul des Weiteren:

einen 2D Barcode erzeugt, indem die Dokumenten-Information verschlüsselt wird, wobei ein Zufalls-Schlüssel verwendet wird; und das Zertifizier-Modul außerdem:
das zertifizierte Dokument erzeugt, welches die Dokumenten-Information und den Zufalls-Schlüssel enthält

- ein Offline Verifizier-Modul, welches auf einem allein operierenden Verifizier-Daten-System läuft, und welches bereitgestellt ist um zumindest:

(i) das zertifizierte Dokument zu empfan-

gen;
(ii) den Zufalls-Schlüssel zu entschlüsseln, wobei der System-Entschlüsselungs-Schlüssel verwendet wird;
(iii) die Dokumenten-Information zu entschlüsseln, wobei der Zufalls-Schlüssel verwendet wird;

dadurch gekennzeichnet, dass das Zertifizier-Modul außerdem: den 2D Barcode erzeugt, indem der Zufalls-Schlüssel verschlüsselt wird, wobei der System-Verschlüsselungs-Schlüssel verwendet wird, wobei der verschlüsselte Zufalls-Schlüssel mit dem System-Entschlüsselungs-Schlüssel entschlüsselt werden kann; und
des Weiteren **gekennzeichnet dadurch, dass** das Offline Verifizier-Modul: die in dem 2D Barcode enthaltene Information anzeigt, wobei die Information den verschlüsselten Zufalls-Schlüssel enthält.

2. System nach Anspruch 1, wobei der 2D Barcode durch die folgenden Schritte erzeugt wird:

(i) Komprimieren der Dokumenten-Information;
(ii) Verschlüsseln der komprimierten Dokumenten-Information mit einem System-erzeugten Zufalls-Schlüssel,
(iii) Verschlüsseln des Zufalls-Schlüssels mit einem System-Verschlüsselungs-Schlüssel vom Hauptmodul, und
(iv) Erzeugen des 2D Barcodes aus dem verschlüsselten Zufalls-Schlüssel und der verschlüsselten komprimierten Dokumenten-Information.

3. System nach Anspruch 2, des Weiteren aufweisend ein Offline Verifizier-Modul, welches bereitgestellt ist um zumindest:

(i) das zertifizierte Dokument zu scannen;
(ii) den Zufalls-Schlüssel zu entschlüsseln, wobei der System-Entschlüsselungs-Schlüssel verwendet wird;
(iii) die komprimierte Dokumenten-Information zu entschlüsseln, wobei der Zufalls-Schlüssel verwendet wird;
(iv) die Dokumenten-Information zu dekomprimieren;
(v) die Dokumenten-Information aus dem 2D Barcode mit weiterer gezeigter Dokumenten-Information zu vergleichen.

4. System nach Anspruch 1, wobei der 2D Barcode durch die folgenden Schritte erzeugt wird:

(i) Komprimieren der Dokumenten-Information;
(ii) Verschlüsseln des komprimierten Dokumenten-Information Hash-Codes mit einem System-Verschlüsselungs-Schlüssel vom Hauptmodul,
(iii) Erzeugen des 2D Barcodes aus dem verschlüsselten Hash-Code und der komprimierten Dokumenten-Information.

5. System nach Anspruch 4, des Weiteren aufweisend ein Offline Verifizier-Modul, welches bereitgestellt ist um zumindest:

(i) das zertifizierte Dokument zu scannen;
(ii) den Zufalls-Schlüssel zu entschlüsseln, wobei der System-Entschlüsselungs-Schlüssel verwendet wird;
(iii) den Hash-Code mit dem System-Entschlüsselungs-Schlüssel zu entschlüsseln;
(iv) den Hash-Code mit dem komprimierten Dokumenten-Information Hash-Code zu vergleichen;
(vi) die Dokumenten-Information zu dekomprimieren;
(v) die Dokumenten-Information aus dem 2D Barcode mit weiterer gezeigter Dokumenten-Information zu vergleichen.

6. System nach einem der Ansprüche 1 bis 5, wobei die Unterschrift durch ein digitales Pad und einen elektronischen Stift registriert wird.

7. System nach einem der Ansprüche 1 bis 6, wobei der Zugriff auf eines der Module **dadurch** gewährt wird, dass eine ID Nummer, ein Paßwort, und eine elektronische Unterschrift eingegeben wird.

8. System nach einem der Ansprüche 1 bis 7, wobei auf mindestens eines der Module über das Internet unter Verwendung eines Internet Browsers zugegriffen werden kann.

9. System nach einem der Ansprüche 1 bis 8, wobei zumindest das Hauptmodul, das Admin Module, und das Registrations-Modul auf dem gleichen Applikations-Server laufen.

10. 2D Barcode zur Zertifizierung und Authentifizierung von Dokumenten-Information, zumindest aufweisend die komprimierte Dokumenten-Information und einen Krypto-Schlüssel zur Verifizierung und/oder Verschlüsselung der Dokumenten-Information.

Revendications

1. Système de certification et d'authentification électronique comprenant les composants suivants :

- un module principal qui autorise l'accès à un module d'administration et qui fournit des données cryptographiques, en particulier une paire

de clés cryptographiques comprenant une clé de chiffrement de système et une clé de déchiffrement de système, à utiliser avec le système ;
- dans lequel le module d'administration est prévu au moins pour :

(i) saisir et stocker des informations sur le bureau de certification ;
(ii) autoriser l'accès au module d'enregistrement en saisissant et en stockant au moins des informations de registraire et au moins une signature électronique de registraire ;
(iii) activer ou désactiver des registraires ;
(iv) fournir à des registraires des identifiants et des mots de passe d'utilisateurs ;

- dans lequel le module d'enregistrement est prévu au moins pour :

(i) saisir des informations sur une entreprise ;
(ii) enregistrer des informations sur un membre de l'entreprise et inscrire des signatures d'un membre ;
(iii) activer ou désactiver des signataires ou des membres de l'entreprise ; et
(iv) fournir au membre de l'entreprise un identifiant et un mot de passe de membre ;

- un module de certification qui est prévu au moins pour :

(i) saisir et sauvegarder les informations de document destinées à la certification ;
(ii) inscrire la signature du membre ; et
(ii) comparer la signature inscrite avec les signatures du membre stocké, dans lequel si la signature inscrite concorde avec les signatures du membre stocké, ledit module de certification doit en outre engendrer un code à barres 2D en chiffrant les informations de document à l'aide d'une clé aléatoire ; et le module de certification doit en outre produire le document certifié incluant les informations de document et la clé aléatoire ;

- un module de vérification hors ligne qui fonctionne sur un système de données de vérificateur autonome, qui est prévu au moins pour :

(i) recevoir le document certifié ;
(ii) déchiffrer la clé aléatoire à l'aide de la clé de déchiffrement du système ;
(iii) déchiffrer les informations du document à l'aide de la clé aléatoire ;

caractérisé en ce que le module de certification doit en outre engendrer le code à barres 2D en chiffrant la clé aléatoire à l'aide de la clé de chiffrement du système, dans lequel ladite clé aléatoire chiffrée est apte à être déchiffrée à l'aide de la clé de déchiffrement du système ;
caractérisé en outre en ce que le module de vérification hors ligne est prévu en outre pour afficher les informations contenues dans le code à barres 2D, les informations comprenant la clé aléatoire chiffrée.

2. Système selon la revendication 1, dans lequel le code à barres 2D est engendré par les étapes suivantes :

(i) compresser les informations de document ;
(ii) chiffrer les informations de document compressées à l'aide d'une clé aléatoire engendrée par le système ;
(iii) chiffrer la clé aléatoire avec une clé de chiffrement de système provenant du module principal ; et
(iv) engendrer le code à barres 2D à partir de la clé aléatoire chiffrée et des informations de documents compressées chiffrées.

3. Système selon la revendication 2, comprenant en outre un module de vérification hors ligne qui est prévu au moins pour :

(i) numériser par balayage le document certifié ;
(ii) déchiffrer la clé aléatoire avec la clé de déchiffrement du système ;
(iii) déchiffrer les informations compressées de document avec la clé aléatoire ;
(iv) décompresser les informations de document ;
(v) comparer les informations de document provenant du code à barres 2D avec les informations d'un autre document montré.

4. Système selon la revendication 1, dans lequel le code à barres 2D est engendré par les étapes suivantes :

(i) compresser les informations de document ;
(ii) chiffrer le code de hachage des informations compressées de document avec une clé de chiffrement du système provenant du module principal ;
(iii) engendrer le code à barres 2D à partir du code de hachage chiffré et des informations compressées de document.

5. Système selon la revendication 4, comprenant en outre un module de vérification hors ligne qui est prévu au moins pour :

(i) numériser par balayage le document certifié ;
(ii) déchiffrer la clé aléatoire avec la clé de déchiffrement du système ;
(iii) déchiffrer le code de hachage avec la clé de déchiffrement du système ;
(iv) comparer le code de hachage avec le code de hachage des informations compressées de document ;
(v) décompresser les informations de document ;
(vi) comparer les informations de document provenant du code à barres 2D avec les informations d'un autre document montré.

6. Système selon l'une quelconque de revendications 1 à 5, dans lequel la signature est inscrite par le biais d'un bloc numérique et d'un stylo électronique.

7. Système selon l'une quelconque des revendications 1 à 6, dans lequel l'accès à l'un des modules est accordé par la saisie d'un numéro d'identification, d'un mot de passe et d'une signature électronique.

8. Système selon l'une quelconque des revendications 1 à 7, dans lequel il est possible d'accéder à au moins l'un des modules sur Internet à l'aide d'un navigateur Internet.

9. Système selon l'une quelconque des revendications 1 à 8, dans lequel au moins le module principal, le module d'administration et le module d'enregistrement fonctionnent sur le même serveur d'applications.

10. Code à barres 2D pour la certification et l'authentification d'informations de document, contenant au moins les informations compressées de document et une clé cryptographique pour la vérification et/ou le chiffrement des informations de document.

FIG.1

FIG.2

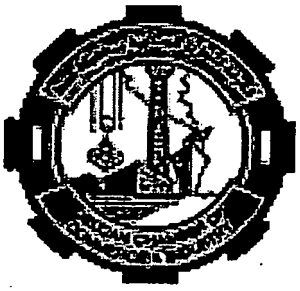

FIG.3

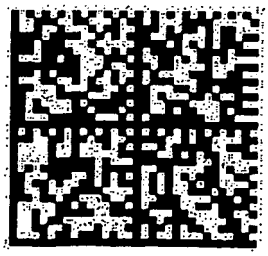

FIG.4