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

(11) EP 1 688 891 A1

(12) EUROPEAN PATENT APPLICATION

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

(51) Int Cl.:
G07D 7/00 $^{(2006.01)}$

(21) Application number: 05002155.9

(22) Date of filing: 02.02.2005

(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

(71) Applicant: Geoffrey, Mohammed A.
21434 Jeddah (SA)

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

(74) Representative: Jehle, Volker Armin et al
Bosch, Graf v. Stosch, Jehle
Patentanwalt GmbH
Flüggenstrasse 13
80639 München (DE)

(54) Electronic certification and authentication system

(57) The invention relates to a certification and authentication system, comprising a Main Module which grants access to the an Admin Module and which provides crypto-data for use with the system, wherein the Admin Module is provided to enter and store certification office information, grant access to the a Registration Module and provide certification office registrars with user IDs and passwords; wherein the Registration Module is provided to enter a companies' information register a companies members' information and enroll member's signatures, activate or deactivate signatories or companies' members; and provide companies' members with their IDs and passwords; and further a Certification Module which is provided to at least enroll the member's signature and compare the enrolled signature with the stored member's signatures and, if the signature is correct, enter and save a document information that needs to be certified and print the certified letter in form of a 2D barcode; and further an Authorization Module which is provided to print the certified letter, and further an Offline Verification Module which is provided to scan the certified document and read the scanned information in the 2D barcode.

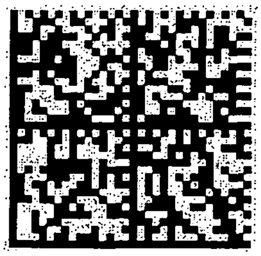

FIG.4

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 one of several modules:

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: a member can use this module to, by the way of an example:

a) Enter and save the document information that needs to be certified;
b) Enroll his signature by the way of, for example, a digital pad and an electronic pen. The system then compares the enrolled signature pattern(s) with the member's signatures pattern(s) stored in the database(s). If the signature is correct, the system displays, e.g. on an intemet browser, at least one of: the member signature, his company stamp, certification office stamp, Certification number, Certification date, Certification time and a 2D barcode;
c) Print the certified letter displayed himself, i.e. a printer connected to his data station / PC;
d) Authorize the printing by another person.

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 that runs on a stand alone verifier data system, e.g. a PC notebook, palm, mobile phone etc., connected to a scanner. The verifier can use this module to esp. do the following:

a) Scanning the certified document with the scanner;
b) Reading the information in the 2D barcode after either:

decrypting the random key with the system decryption key, and
decrypting the compressed document information with the random key
or: decrypting the hash code with the system decryption key and
comparing it with compressed document information Hash code);

c) Decompressing the document information and displaying it;
d) Comparing and/or printing the information displayed to verify its correctness and safety from fraud.

[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] It is understood that this exemplary description does not limit the scope of the invention.

[0007] The modules of this invention are linked to each other and preferably share one database, and work as one system.

[0008] 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.

[0009] 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.

[0010] 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.

[0011] 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.

[0012] 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.

[0013] 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.

[0014] 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, for example:

- ■ 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.

or by:

- ■ encrypting the compressed document information Hash code with the system encryption key, generating the 2D barcode from the encrypted Hash code and the compressed document information.

[0015] The encryption key is preferably one key out of a key pair, as for example from a asymmetric encription algorithm (e.g. PKI).

[0016] 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.

[0017] The Offline Verification Module enables verifiers to read the 2D barcode after scanning the document and to display the corresponding information.

[0018] The decryption can be carried out by, for example:

- ■ decrypting the random key by the system decryption key, decrypt the compressed document information using the random key

or by

- ■ decrypting the hash code with the system decryption key and comparing it with the compressed document information hash code,

resp. 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.

[0019] 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 the 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 registrars' information and registrar's at least one electronic signature;
  (iiii) activate or deactivate registrars;
  (iv) provide registrars with user IDs and passwords;

- wherein the Registration Module is provided to at least:

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

- a Certification Module which is provided to at least:

  (i) enroll the member's signature and compare the enrolled signature with the stored member's signatures and, if the signature is correct, enter and save a document information that needs to be certified;
  (iii) print the certified letter in form of a 2D barcode;

- an Authorization Module which is provided to at least:

(i) print the certified letter;

- an Offline Verification Module which is provided to at least:

(i) scan the certified document; and
(ii) read the scanned information in the 2D barcode.

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 intemet using an intemet 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.

FIG.1

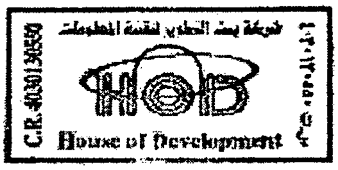

FIG.2

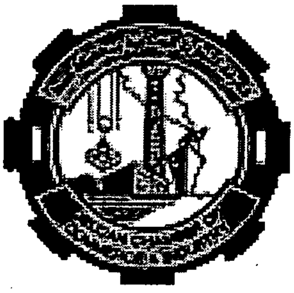

FIG.3

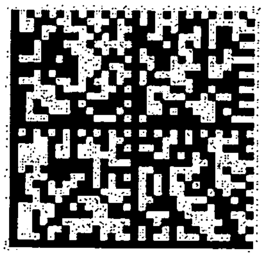

FIG.4

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 05 00 2155

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	US 2002/023220 A1 (KAPLAN JONATHAN C) 21 February 2002 (2002-02-21) * abstract * * paragraph [0087] * * paragraphs [0010] - [0019] * -----	1-10	G07D7/00

TECHNICAL FIELDS SEARCHED (IPC)

G07D
H04L

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	6 February 2006	Mennerun, S

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO.

EP 05 00 2155

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

06-02-2006

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2002023220 A1	21-02-2002	AU 8830901 A	04-03-2002
		WO 0217539 A2	28-02-2002

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82