



(51) International Patent Classification:

G06F 21/20 (2006.01) H04L 9/28 (2006.01)
G06F 21/24 (2006.01)

(21) International Application Number:

PCT/MY2010/000304

(22) International Filing Date:

29 November 2010 (29.11.2010)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

PI 2010004936 20 October 2010 (20.10.2010) MY

(71) Applicant (for all designated States except US): **MIMOS BERHAD** [MY/MY]; Technology Park Malaysia, 57000 Kuala Lumpur (MY).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **SEA CHONG Seak** [MY/MY]; Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). **TAN FUI Bee** [MY/MY]; Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). **NG KANG Siong** [MY/MY]; Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). **GALOH RASHIDAH Haron** [MY/MY]; Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). **TAN SOO Sian** [MY/MY]; Mimos Berhad, Tech-

nology Park Malaysia, 57000 Kuala Lumpur (MY). **NOR IZYANI Daud** [MY/MY]; Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY).

(74) Agent: **MIRANDAH, Patrick**; Patrick Mirandah CO. (malaysia) SDN BHD, Suite 3B-19-3 Plaza Sentral, Jalan Stesen Sentral 5, 50470 Kuala Lumpur (MY).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: A METHOD FOR CREATING AND VERIFYING DIGITAL SIGNATURE IN A SERVER

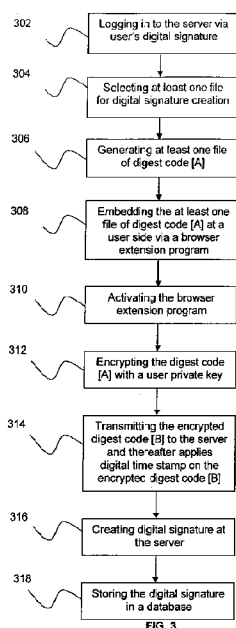


FIG. 3

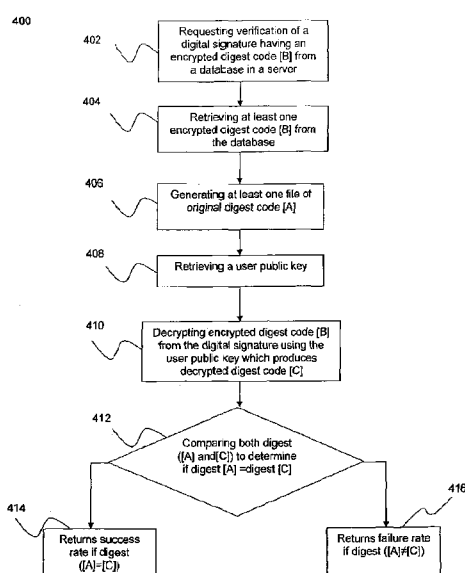


FIG. 4

(57) Abstract: One embodiment of the present invention provides a method (300) for creating digital signature in a server, the method comprising the steps of logging in to the server via user's digital certificate (302), selecting at least one file for digital signature creation (304), generating at least one file of digest code [A] (306), embedding the at least one file of digest code [A] in a browser extension program at client side (308), activating the browser extension program (310), encrypting the digest code [A] with a user private key (312), transmitting the encrypted digest code [B] to the server (314), creating a digital signature at the server (316) and storing the digital signature in a database (318). Another embodiment of the present invention provides a method (400) for verifying digital signature in a server, the method comprising the steps of requesting verification of a digital signature having an encrypted digest code [B] from a database in a server (402), retrieving at least one encrypted digest code [B] from the database (404), generating at least one file of original digest code [A] (406), retrieving a user public key (408), decrypting encrypted digest code [B] from the digital signature using the user public key which produces decrypted digest code [C] (410) and comparing both digest ([A] = [C]) (412) to determine a success or failure rate of the decrypted information.

user public key which produces decrypted digest code [C] (410) and comparing both digest ([A] = [C]) (412) to determine a success or failure rate of the decrypted information.

**Declarations under Rule 4.17:****Published:**

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))* — *with international search report (Art. 21(3))*

-1-

A METHOD FOR CREATING AND VERIFYING DIGITAL SIGNATURE IN A SERVER

FIELD OF INVENTION

- 5 The present invention relates to a method for creating and verifying digital signature in a server by maintaining the user private key at the client side.

BACKGROUND ART

10 Digital signature provides the means for an electronic document (e.g. e-mail, spreadsheet, text file, etc.) to be authenticated. Digital signatures rely on certain encryption methodologies to ensure authentication between two or more parties entering into a transaction over the network. Typical file based digital signature type software application always performed as non web based application due to user private key store in hardware token at client computer, such as smart card, USB token and etc.

15 At present, the main problem encountered during the digital signing process is where the user private key is stored in any hardware token at remote client side and the document(s) must reside in the server without transmitting it out. The user's private keys are not recommended to be deposited at any server while transmission across network is not allowed in respect of security issues.

20

The present invention provides a methodology for creating and verifying digital signature at the server side while maintaining the user private key at the client side. The user's private key remains at the client computer during the digital signature process wherein transmission of private key to the server is not allowed. A browser extension program is provided in the present invention wherein the browser extension program customizes the digital signing process at the client side wherein the private key resides in the client side.

25

The subject matter claimed herein is not limited to embodiments that solve any disadvantages or that operate only in environments such as those described above. Rather, this background is only provided to illustrate one exemplary technology area where some embodiments described herein may be practice.

30

SUMMARY OF INVENTION

One aspect of the present invention is a method for creating digital signature in a server by maintaining the user private key at the client side. The method comprising the steps of logging in to server via user's digital certificate (302); selecting at least one file for digital signature creation (304), generating at least one file of digest code [A] (306), embedding the at least one file of digest code [A] in a browser extension program at client side (308), activating the browser extension program (310), encrypting the digest code [A] with a user private key (312), transmitting the encrypted digest code [B] to the server (314) and creating a digital signature at the server (316). Thereafter, the digital signature is stored in a database (318). The method for transmitting the encrypted digest code [B] to the server (314) further comprises applying digital time stamp for creation of the digital signature.

15 The user private key is maintained at the user and/or client side. The user private key which is maintained at the user and/or client side is not allowed to be transmitted to the server.

Another aspect of the present invention is a method (400) for verifying digital signature in a server. The method comprising the steps of requesting verification of a digital signature having an encrypted digest code [B] from a database in a server (402), retrieving at least one encrypted digest code [B] from the database (404), generating at least one file of original digest code [A] (406), retrieving a user public key (408), decrypting encrypted digest code [B] from the digital signature using the user public key which produces decrypted digest code [C] (410) and comparing both digest ([A] = [C]) (412). The method of comparing both digest ([A] = [C]) further comprises determining the success status rate and failure status rate wherein information indicative of a signature element returns a success status rate when digest code [A] matches digest code [C] in signature data (414). Else information indicative of a signature element returns a failure status rate when digest code [A] does not match digest code [C] in signature data (416).

The success rate indicates that files received has not been tampered or modified while the failure status rate indicates that files received has been tampered or modified.

-3-

The present invention consists of features and a combination of parts hereinafter fully described and illustrated in the accompanying drawings, it being understood that various changes in the details may be made without departing from the scope of the invention or sacrificing any of the advantages of the present invention.

BRIEF DESCRIPTION OF ACCOMPANYING DRAWINGS

To further clarify various aspects of some embodiments of the present invention, a more particular description of the invention will be rendered by references to specific
5 embodiments thereof, which are illustrated in the appended drawings. It is appreciated that these drawings depict only typical embodiments of the invention and are therefore not to be considered limiting of its scope. The invention will be described and explained with additional specificity and detail through the accompanying drawings in which:

10 FIG. 1 illustrates a sequence diagram of digital signature creation in a server.

FIG. 2 illustrates a sequence diagram of digital signature verification in a server.

FIG. 3 is a flowchart illustrating a method for creating digital signature in a server.

15

FIG. 4 is a flowchart illustrating a method for verifying digital signature in a server

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The invention relate to a method for creating and verifying digital signature in a server by maintaining the user private key at the client side. Hereinafter, this specification will describe the present invention according to the preferred embodiments. It is to be understood that limiting the description to the preferred embodiments of the invention is merely to facilitate discussion of the present invention and it is envisioned without departing from the scope of the appended claims.

Reference is first being made to FIG. 1 and FIG. 3 respectively. FIG. 1 illustrates a sequence diagram of digital signature creation in a server while FIG. 3 is a flowchart illustrating a method for creating digital signature in a server. FIG. 1 illustrates the interaction between the client side and the server side (client-server system) via a browser extension program for digitally signing data. Browser extension program which is a browser add-ons which is also known as extensions is a small (mini) computer program that extends the functionality of a browser to perform and customize the digital signing process at the user side. Browser extension program generally enhances the default functionality of the web browser.

The user first log in to a server using user's digital certificate via server side scripting in a server side channel (302) and the user first selects at least one file for digital signature creation (304). Thereafter, the server generates at least one file of digest code [A] (306). Digest codes are data generated for encoding purposes wherein the digest code includes hash value returned by a hash function. The said data is often referred to as "message", "message digest" or simply "digest". At least one file of digest code is embedded in the browser extension program at client side (308). The browser extension program is activated (310) to enable the functionality as described above to allow the transmission of the digest code to the user side. Subsequently, the digest code [A] is encrypted with a user private key (312) wherein the user private key maintains at the user and/or client side. The user private key which is maintained at the user and/or client side is not allowed to be transmitted to the server for protection of data and to avoid data losses via eavesdropping in the network, etc.

The encrypted digest code also known as digest code [B] is thereafter transmitted from client side to the server (314) to create a digital signature (316) which will be stored in a

-6-

database (318). The digital signature which is created by encrypting digest code [A] with the user private key which resides at the user and/or client side is further stamped wherein digital time stamp is applied for creation of the digital signature. Therefore, the digitally signed data comprises of digest code [B] which is digitally stamped. Digital time stamp creates a unique identifier wherein time stamping presents data in a consistent format.

Reference is now being made to FIG. 2 and FIG. 4 respectively. FIG. 2 illustrates a sequence diagram of digital signature verification in a server while FIG. 4 is a flowchart illustrating a method for verifying digital signature in a server. FIG. 2 illustrates the interaction between the client side and the server side (client-server system) via a browser extension program for verifying the digitally signed data.

The user first logs in to a server using user's digital certificate via server side scripting in a server side channel for verification of the digitally signed signature. Upon successful log-in to the server, the user first request for verification of a digital signature having an encrypted digest code [B] from a database in the server (402). Thereafter, the server retrieves at least one encrypted digest code from the database (404). Subsequently, the server generates at least one file of original digest code [A] (406). The user public key is retrieved (408) to enable decryption of encrypted digest code [B] from the digital signature to obtain decrypted digest code [C] (410). Upon successful decryption of the encrypted digest code [B] via a user public key, both digest code [A] and digest code [C] is compared (412) to determine data integrity wherein success status rate indicates that files received has not been tampered or modified. Failure status rate indicates that files received has been tampered or modified.

The success status rate of the decrypted digest code [C] is determined when digest code [A] matches digest code [C] in the signature data (414) and the failure status rate of the decrypted digest code [C] is determined when digest code [A] does not match digest code [C] in the signature data (416).

The methodology of the digital signature service which provides for creating and verifying digital signature in a server operates as a web-based application. The said

-7-

methodology provides for user private key which resides at the client side at all times to ensure protection of data integrity as the user private key will not be disclosed.

5 The present invention may be embodied in other specific forms without departing from its essential characteristics. The described embodiments are to be considered in all respects only as illustrative and not restrictive. The scope of the invention is, therefore indicated by the appended claims rather than by the foregoing description. All changes, which come within the meaning and range of equivalency of the claims, are to be embraced within their scope.

CLAIMS

1. A method (300) for creating digital signature in a server, the method comprising the steps of:
 - 5 logging in to the server via user's digital certificate (302)
selecting at least one file for digital signature creation (304);
generating at least one file of digest code [A] (306);
embedding the at least one file of digest code [A] in a browser extension
program at a client side (308);
10 activating the browser extension program (310);
encrypting the digest code [A] with a user private key (312);
transmitting the encrypted digest code [B] to the server (314);
creating a digital signature at the server (316);
storing the digital signature in a database (318);
15 characterized in that
transmitting the encrypted digest code [B] to the server (314)
further comprises applying digital time stamp for creation of the
digital signature.
- 20 2. The method according to Claim 1, wherein the at least one file of digest code includes hash value returned by a hash function.
3. The method according to Claim 1, wherein the digital time stamp generates a
unique identifier in creating the digital signature.
- 25 4. The method according to Claim 1, wherein the user private key maintains at the
user and/or client side.
5. The method according to Claim 4, wherein the user private key is maintained at
30 the user and/or client side is not allowed to be transmitted to the server.

6. The method according to Claim 4, wherein the method for creating digital signature in a server includes creation of digital signature for a web-based application.
- 5 7. A method (400) for verifying digital signature in a server, the method comprising the steps of:
- requesting verification of a digital signature having an encrypted digest code [B] from a database in a server (402);
- retrieving at least one encrypted digest code [B] from the database (404);
- 10 generating at least one file of original digest code [A] (406);
- retrieving a user public key (408);
- decrypting encrypted digest code [B] from the digital signature using the user public key which produces decrypted digest code [C] (410);
- comparing both digest ([A] and [C]) (412);
- 15 information indicative of a signature element returns a success status rate when digest code [A] matches decrypted digest code [C] in signature data (414); else
- information indicative of a signature element returns a failure status rate when digest code [A] does not match decrypted digest code [C] in
- 20 signature data (416).
8. The method according to Claim 7, wherein the success status rate indicates that files received has not been tampered or modified.
- 25 9. The method according to Claim 7, wherein the failure status rate indicates that files received has been tampered or modified.
10. The method according to Claim 7, wherein the method for verifying digital signature in a server includes verification of digital signature for a web-based
- 30 application.

1/4

100

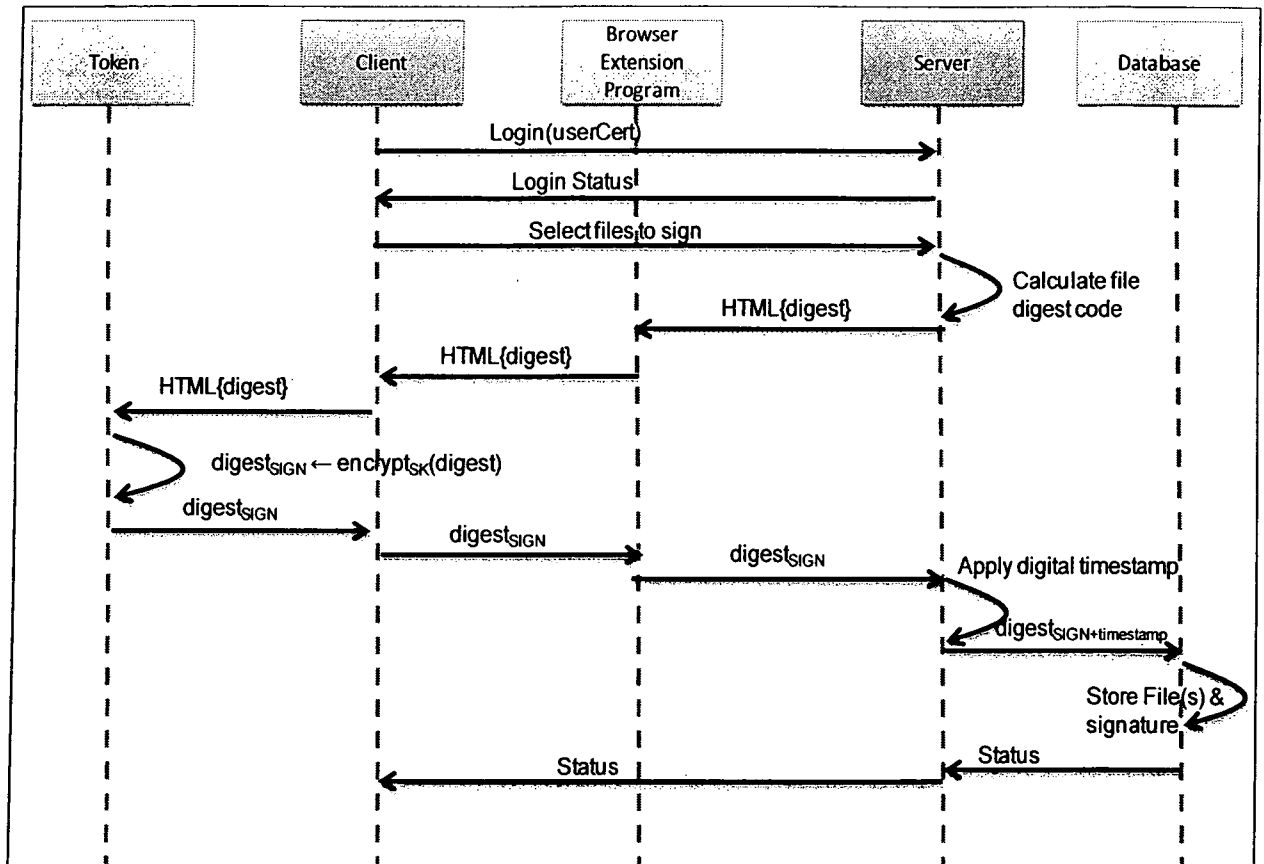


FIG.1

200

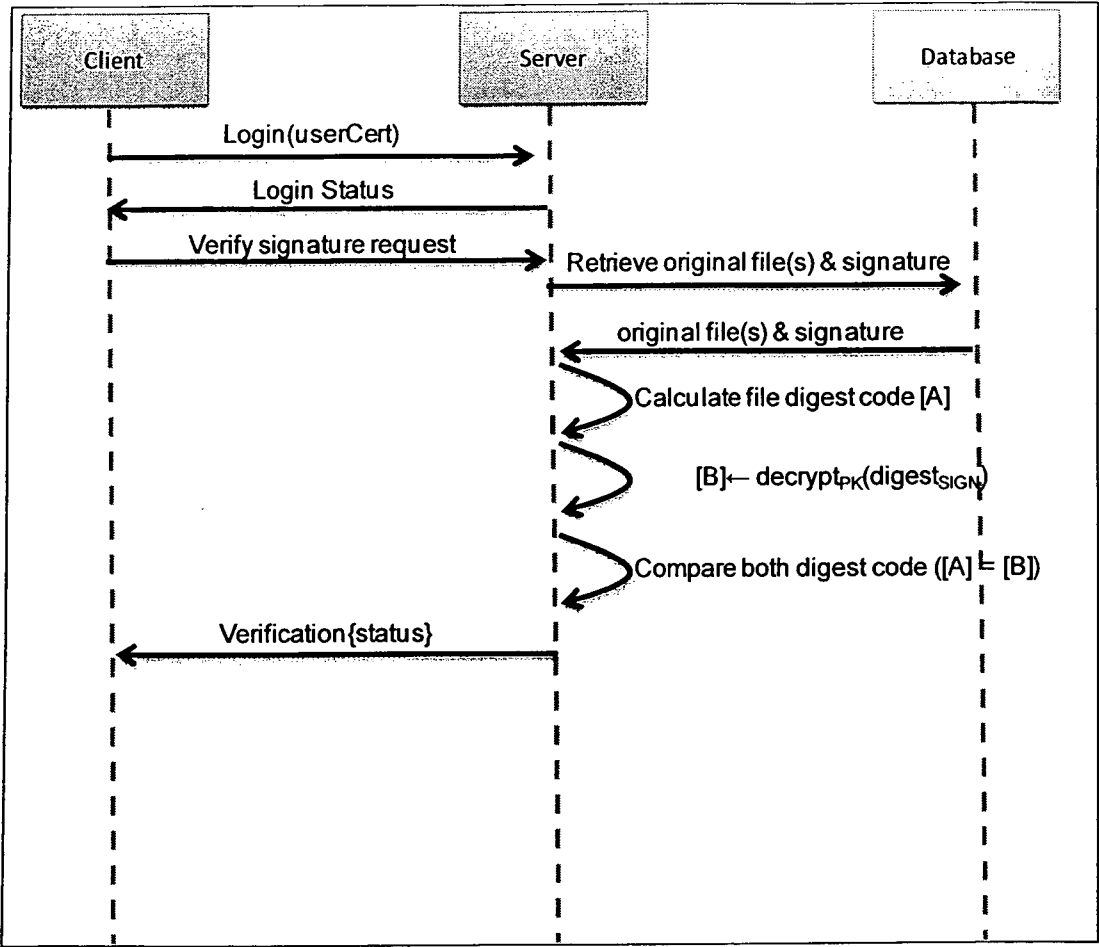


FIG. 2

3/4

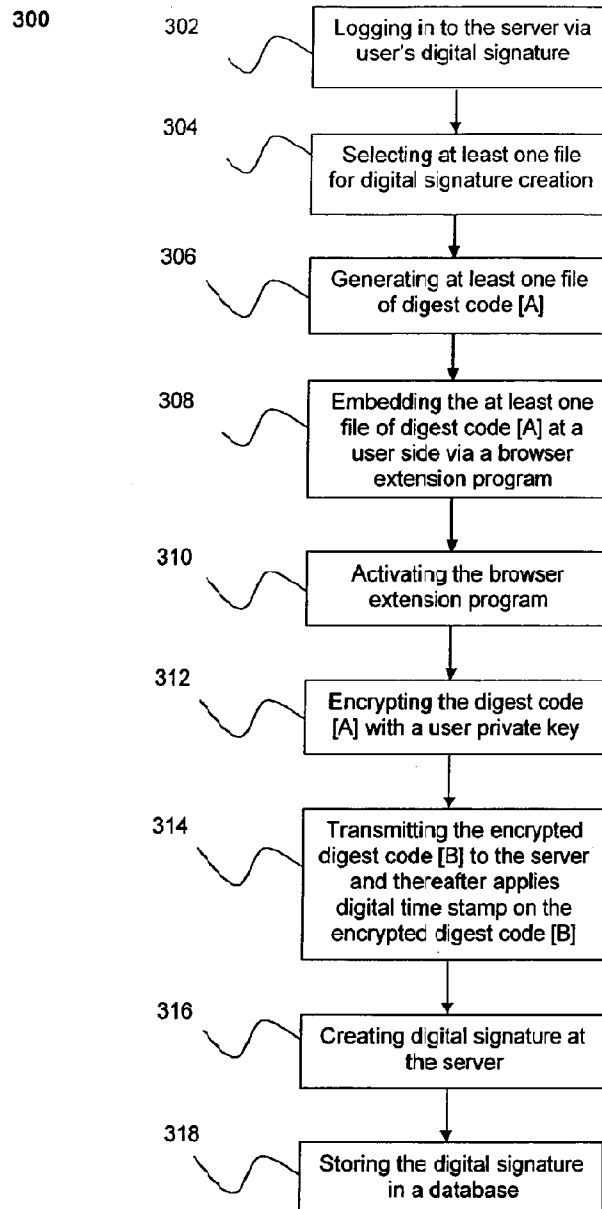


FIG. 3

4/4

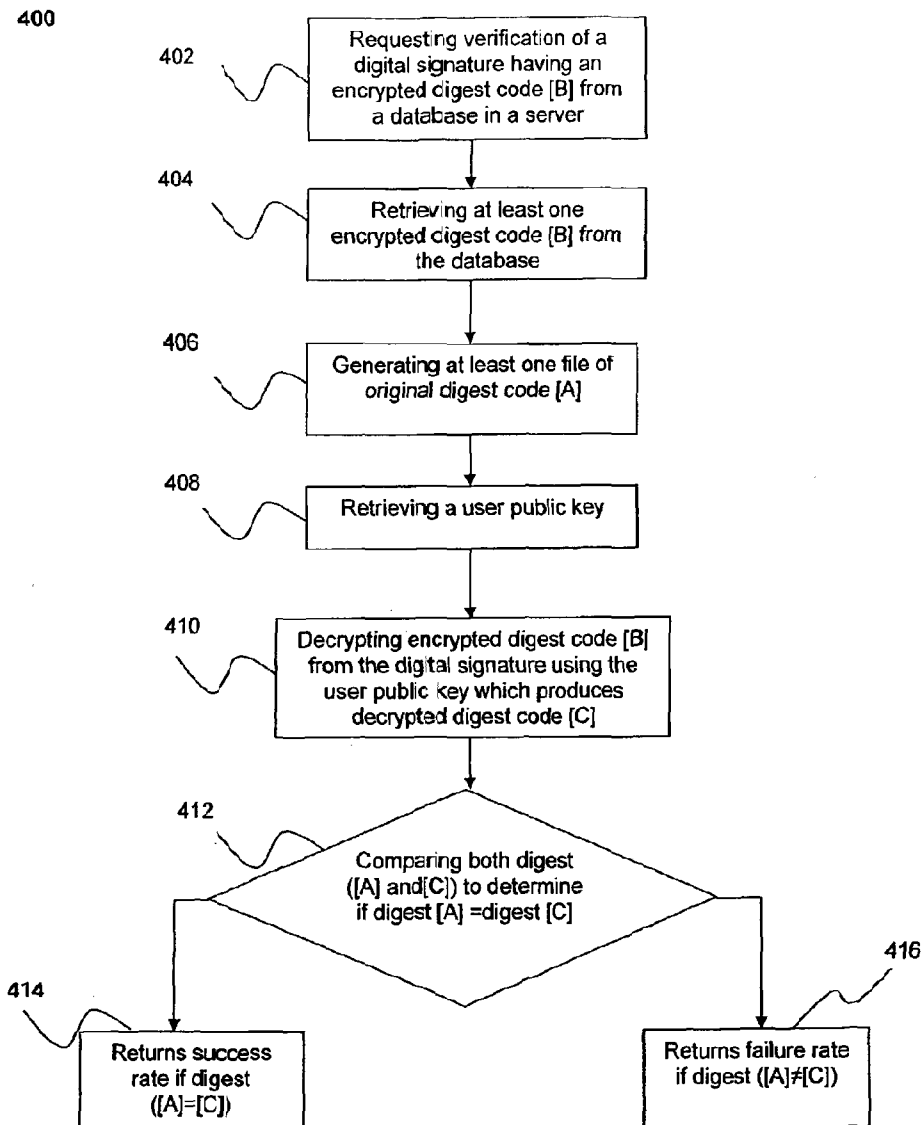


FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/MY2010/000304**A. CLASSIFICATION OF SUBJECT MATTER****G06F 21/20(2006.01)i, G06F 21/24(2006.01)i, H04L 9/28(2006.01)i**

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F 21/20; G06F 21/24; H04L 9/08; G09C 1/00; G06F 12/14; H04L 9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS(KIPO internal) & Keywords: ((<word>g06f21) <in> IPC)<AND>(((encrypt <and> key <and> server <and> store <and> file) <in> AB))

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2010-0138656 A1 (CHINEN MITSURU et al.) 03 June 2010 See abstract & claims	1-10
A	US 2010-0185852 A1 (OGAWA TOMOYUKI et al.) 22 July 2010 See abstract & claims	1-10
A	JP 2008-250369 A (SORUN CORP) 16 October 2008 See abstract & claims	1-10

☐ Further documents are listed in the continuation of Box C.☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

21 NOVEMBER 2011 (21.11.2011)

Date of mailing of the international search report

22 NOVEMBER 2011 (22.11.2011)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
Government Complex-Daejeon, 189 Cheongsu-ro,
Seo-gu, Daejeon 302-701, Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

UHM, In Kwon

Telephone No. 82-42-481-5712



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/MY2010/000304

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2010-0138656 A1	03.06.2010	CA 2738466 A1 EP 2345977 A1 KR 10-2011-0096554 A WO 2010-061801 A1	03.06.2010 20.07.2011 30.08.2011 03.06.2010
US 2010-0185852 A1	22.07.2010	CN 101484927 A EP 2043073 A1 WO 2009-004732 A1	15.07.2009 01.04.2009 08.01.2009
JP 2008-250369 A	16.10.2008	None	