



(51) International Patent Classification:

G06F 21/64 (2013.01)

(21) International Application Number:

PCT/MY2014/000067

(22) International Filing Date:

22 April 2014 (22.04.2014)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

PI 2013002270 18 June 2013 (18.06.2013) MY

(71) Applicant: MIMOS BERHAD [MY/MY]; Technology Park Malaysia, 57000 Kuala Lumpur (MY).

(72) Inventors: MOHAMAD, Moesfa Socheila Binti; c/o MIMOS Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). POH, Geong Sen; c/o 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, BN, 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, IR, IS, JP, KE, KG, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, 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, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, 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, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

- as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))
- of inventorship (Rule 4.17(iv))

Published:

- with international search report (Art. 21(3))

[Continued on next page]

(54) Title: NON-REPUDIABLE COLLABORATIVE UPDATES OF DOCUMENT

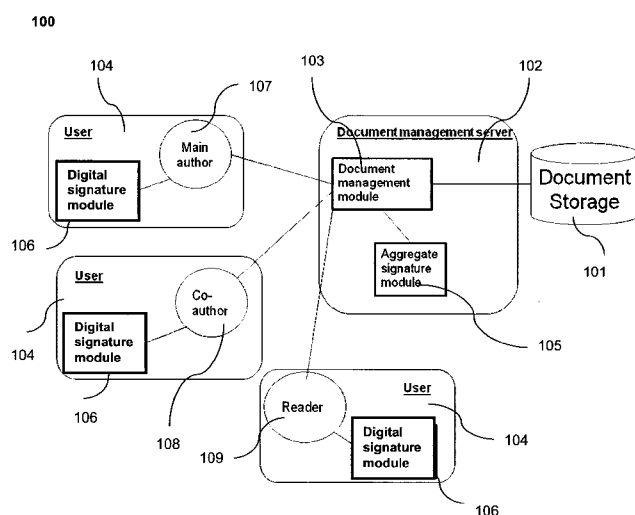


Figure 1.0

(57) Abstract: A system for collaborative document generation comprising: a document management server (102) adapted to manage document storage (101) and having an associated pair of signing and verification keys; at least two clients (104) each having a unique identifier and a pair of signing and verification keys, said verification keys of said clients being available to said document management server and to other clients; a document management module (103) adapted to receive service requests from said clients; an aggregate signature module (105) residing in said document management server; and digital signature modules (106) residing in each of said clients; wherein said aggregate signature module is adapted to: sign messages using the document management server signing key; verify signatures on messages given a signature, verification key and message; aggregate a set of signatures to produce an aggregate signature; and verify said aggregate signature given said aggregate signature, a set of associated verification keys and a set of associated messages; and wherein said digital signature modules are adapted to: sign messages using the respective client signing keys; verify signatures and messages given a signature, verification key and message; and verify said aggregate signature given said aggregate signature, a

set of associated verification keys and a set of associated messages.



-
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

NON-REPUDIABLE COLLABORATIVE UPDATES OF DOCUMENT

FIELD OF INVENTION

5 The present invention relates to a system and method for collaborative document creation. In particular, the invention relates to systems and methods that facilitate aggregation of signatures validly created by more than one contributor to the collaborative document.

10 BACKGROUND ART

Workplaces are generally moving more and more towards an almost paperless working environment. As this process evolves, every aspect of workflow and procedure generally requires its own digital counterpart. It is generally preferred, and in some instances
15 required, that the digital workflow and procedure adopted maintains workflow, improves completion times and achieves the same objectives and security levels as its physical counterpart. In the collaborative creation of documents, signatures on the digital counterpart of the document advantageously bind the identity of the signer to the exact content he or she is agreeing to, endorsing and/or approving in such a way that
20 generally no other person will be able to produce the same signature.

There are currently a number of applications available that enable collaborative authoring of documents, for example GoogleDoc and WorkMail (Davide Gazzè, Mariantonietta N. La Polla, Andrea Marchetti, Maurizio Tesconi, Andrea Vivaldi,
25 "WorkMail: Collaborative Document Workflow management by Email", 9th International Cooperative Design Visualisation and Engineering 2012, 2-5 September, 2012). In these applications, an authorization list is maintained through which workflow is realised.

Digital signatures have been widely employed for approval or agreement of documents.
30 In addition, digital signatures have been used to provide authenticity of authorship of documents. Currently, the latter use of digital signatures generally involves a single author signing the entire document to indicate that he or she takes responsibility for its contents. Using such a process, collaborative document creation fails to meet the

authorship commitments achieved in the analogue world, that being where every author signs their signature on the paper. As such, current methods generally involve physical signing of the document by the co-authors or contributors and scanning the papers to create a digital copy of the document.

5

For applications where the document has been defined by sections with authorization defined by those sections, the solution seems clear. Every time a user edits a section the user must sign the section before checking the document back into the server. It follows that when a user wants to read the document the reader should first verify all section signatures to be assured of the authenticity of the document.

10

This invention utilizes an aggregate signature scheme to provide the same assurance with better performance. The aggregate signature scheme enables signatures created by different contributors on different messages to be aggregated into one signature in such a way that if each individual signature is valid, the aggregate signature is also valid with respect to the set of corresponding verification keys. An instance of an aggregate signature scheme is described in Craig Gentry, Zulfikar Ramzan, "Identity-based Aggregate Signatures", Public Key Cryptography (PKC) 2006, LNCS 3958, pp.257-273, 2006.

15

20

An object of the present invention is to provide a system and method that facilitates refined, by section, nonrepudiation of document authorship while maintaining the capability to verify document integrity and authorship of the document as a whole.

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.

SUMMARY OF INVENTION

The present invention relates to a system and method for collaborative document creation. In particular, the invention relates to systems and methods that facilitate
5 aggregation of signatures validly created by more than one contributor to the collaborative document.

One aspect of the present invention provides a system for collaborative document creation comprising at least one document management server (102) adapted to
10 manage document storage (101) and having an associated pair of signing and verification keys; at least two clients (104) each having a unique identifier and a pair of signing and verification keys, the verification keys of the clients being available to the document management server and to other clients; at least one document management module (103) adapted to receive service requests from the clients; at least one
15 aggregate signature module (105) residing in said document management server; and a corresponding number of digital signature modules (106) residing in each of the clients; wherein said aggregate signature module (105) produces one aggregate signature to verify sections of the whole document. The said aggregate signature further comprises steps of signing messages using the document management server signing key;
20 verifying signatures and messages given a signature, verification key and message; aggregating a set of signatures to produce an aggregate signature; and verifying said aggregate signature given the aggregate signature, a set of associated verification keys and a set of associated messages. The corresponding number of digital signature modules having means for signing messages using the respective client signing keys;
25 verifying signatures on messages given a signature, verification key and message; and verifying said aggregate signature given the aggregate signature, a set of associated verification keys and a set of associated messages.

Another aspect of the invention provides a system wherein interactions between the
30 clients and the document management server are conducted over an authenticated channel.

A further aspect of the invention provides a system wherein the document storage (101) is located on a storage server connected to the document management server (102).

Yet another aspect of the invention provides a system wherein the document management module (103) is adapted to store and extract documents from the storage server (102).

Another aspect of the invention provides a system wherein the document management module (103) is located on the document management server (102).

Still another aspect of the invention provides a system wherein the client verification keys are stored in the document management server or in a separate repository that is accessible to the document management server and the clients.

A further aspect of the invention provides a method (250) for non-repudiable updates of document comprising steps of creating collaborative document (252); updating collaborative document (254); and verifying document integrity (256). The step of updating collaborative document further comprises verifying only one aggregate signature to verify sections of the whole document.

Another aspect of the invention provides a method (300) for creating collaborative document which further comprises steps of a user creating a document with defined sections (301); the user signing each of the defined sections to form a list of section signatures (302); the user creating an authorisation list and signing the authorization list (303, 304); the user sending the document, the authorization list, the list of section signatures and the authorisation list signature to at least one document management server (305); the document management server aggregating signatures in the list of section signatures to form a document signature (306); the document management server verifying the document with the document signature (307); the document management server verifying the authorisation list with the authorisation list signature (309); the document management server sending the document signature to the user (310); the user hashing the document and signing a string containing the hash of the document, the document signature and the authorisation list signature to form document integrity information (311); the user sending the document integrity information to the

document management server (312); the document management server verifying the document integrity information (313); and the document management server storing the document, the authorisation list, the list of section signatures; the document signature, the document integrity information and a user identifier (314).

5

Yet another aspect of the invention provides a method comprising updating collaborative document by a client sending a document extraction request with a user identifier to the document management server (501); the document management server verifying the document integrity information (501a); the document management server
10 verifying the document signature (502); the document management server verifying the authorisation list signature (503); the document management server checking whether the user identifier is included in the authorisation list (505); if the user identifier is included in the authorisation list, the document management server sending an editable form of the document to the user together with the document signature (506); the user
15 verifying the document signature (507); the user updating a section of the document to form an updated document (508); the user signing the updated section of the updated document appended with the user identifier and current timestamp to form a new section signature (509); the user sending the updated document and new section signature to the document management server (510); the document management server confirming
20 with the authorisation list that the user is authorised to update the section (511); the document management server verifying the new section signature (513); the document management server updating the list of section signatures (515) and aggregating the signatures to form a new document signature (516); said document management server verifying said new document signature (517); the document management server sending
25 the new document signature and the authorisation list signature to the user (518); the user hashing the updated document and signing a string containing the hash of the document, the new document signature and the authorisation list signature to form new document integrity information; the user sending the document integrity information to the document management server (519); the document management server verifying
30 the new document integrity information (520); and the document management server storing the updated document, the authorisation list; the updated list of section signatures; the new document signature, the new document integrity information and a user identifier (521).

Yet another aspect of the invention provides a method wherein the authorisation list comprises at least the name of the document, a list of all sections of the document, a list of users authorised to update each section of the document and a static content of the document.

5

Still another aspect of the invention provides a method wherein the static content of the document is the hash of the list of all sections of the document.

Yet another aspect of the invention provides a method (800) wherein verification of the document by the document management server comprises verifying the document integrity information (811); and if verified, verifying said document signature (813) or if not verified, stopping said method (812).

A further aspect of the invention provides a further method (900) for creating collaborative document wherein document is hashed (902) and said document hash, document signature and authorization list signature is concatenated (904); signing string (906) and sending signature to server (908); concatenating said document hash, document signature and authorization list signature at server (910); verifying user signature on said string (912); signing said string (914) and combining user's signature and server's signature (916); deleting user's signature and server's signature (918); and combining server verification key and user's verification key (920).

Another aspect of the invention provides a method (700) wherein verifying the document integrity information by the document management server comprises hashing the document (721); extracting the document signature and the authorisation list signature (722); forming a string containing the document hash, the document signature and the authorisation list signature (723); inputting to a digital signature module associated with a client of a user the document integrity information and the formed string and a user verification key associated with a user whose user identifier is in the document integrity information (724); and taking the output of the module as the result (725).

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 the system for collaborative document creation of an embodiment of the invention.

FIG. 2 illustrates the document structure in storage of an embodiment of the invention.

15 FIG. 2A illustrates the general method of the present invention.

FIG. 3 illustrates the document creation process of an embodiment of the method for collaborative document creation of the invention.

20 FIG. 4 illustrates a protocol diagram for the document creation process.

FIG. 5 illustrates the document update process of an embodiment of the method for collaborative document creation of the invention.

25 FIG. 6 illustrates a protocol diagram for the document update process.

FIG. 7 illustrates the process of creating and verifying document integrity information.

FIG. 8 illustrates document verification process flow.

30

FIG. 9 illustrates the steps of a further method for creating collaborative document.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention provides a system and method for collaborative document creation. In particular, the invention relates to systems and methods that facilitate aggregation of signatures validly created by more than one contributor to the collaborative document.

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.

Referring to Figure 1, a system 100 for collaborative document creation is provided. The system 100 includes a storage server 101 connected to a document management server 102. The document management server 102 runs a document management module 103 which users interact with through user 104 to obtain services. The document management module 103 receives requests from users and replies to them following defined methods for each request. As such, the document management module 103 is the module which executes the access control as defined by a main author of a document. In processing requests, the document management module 103 may store or extract documents from the storage server, and interact with other modules in the document management server 102 for specific functions.

The document management server 102 includes an aggregate signature module 105. The aggregate signature module 105 on the document management server 102 produces one aggregate signature to verify sections of the whole document. The aggregate signature module 105 further comprises steps of signing a message: using a signing key of the server to sign a given message; verifying a single signature and message: given a signature, a verification key, and a message, the aggregate signature module 105 returns Success if the signature is valid on the message and verification key. Otherwise it outputs Fail; aggregating a set of signatures: this action produces one signature, that is a document signature; and verifying aggregate: given an aggregate signature, that is a document signature, a set of verification keys and a set of messages,

the aggregate signature module 105 outputs Success if every message is signed with the corresponding signing key of the given set of verification keys. Otherwise it outputs Fail.

- 5 On the clients 104 of the system 100 which are used by the users, there are digital signature modules 106 for signing a message: using signing keys of the users to sign a given message; verifying a single signature and message: given a signature, a verification key, and a message, the digital signature modules 106 return Success if the signature is valid on the message and verification key. Otherwise they output Fail; and
- 10 verifying aggregate: given an aggregate signature, that is a document signature, a set of verification keys and a set of messages, the digital signature modules 106 output Success if every message is signed with the corresponding signing key of the given set of verification keys. Otherwise they output Fail.
- 15 The document management server 102 and users must have a pair of signing and verification keys, and the users must be registered with the system 100 such that the document management server 102 knows every user's unique identifier and verification key. The users' verification keys can be stored in the document management server 102 or in a specialized repository which can be accessed by the document management
- 20 server 102 and all users. The method of generating the key pairs and obtaining users' verification key is not considered within the scope of this invention.

As will be discussed in more detail below, the users of the system 100 may be divided into different categories as said users may take up different roles in the system. For

25 example, the initiator of the document to be created may be considered the main author 107. The main author 107 establishes the document on the system 100 and rules governing the document and its alteration. Those who will be involved in the updating of the document, that is those who will be authorised to make changes to the document, may be considered co-authors 108. It is also envisaged that other parties may have

30 access to the document, but as a read only copy. Such parties may be considered readers 109 of the document.

Referring briefly to Figure 2, the document structure in storage 200 is illustrated. The document 201 includes a number of sections, generally as identified by the main author 107. An authorisation list 202 provides a listing of the sections of the document 200 and the users authorised to make alterations to each section of the document 200. As will be
5 discussed in more detail below, on making alterations to the relevant section of the document 200, signatures of the users 203 are obtained and those signatures are aggregated 204 to obtain a document signature 205. The document signature 205, together with a hash of the document 206 and an authorisation list signature 207 are used to form document integrity information 208.

10

The system 100 and methods of using the system 100 provide for creation and storage of documents and updating of documents by designated co-authors 108. Both methods, those being the creation and storage of documents and updating of documents, are designed to allow more than one users access to collaboratively write a document while
15 maintaining authorization control and providing assurance of authorship. As will be discussed in more detail below, using an aggregate signature, the verification of documents requires verification of only one aggregate signature, instead of one signature per section or one signature per author. In addition, the aggregate signature of the document can be updated by the document management server 102 as one section
20 is updated by a co-author 108 without involving other co-authors 108.

Referring to Figure 2A, a general method for non-repudiable updates of document of the present invention is illustrated. The collaborative document is first created (252). Thereafter, the said collaborative document is updated and the document signature is
25 updated accordingly (254). Further, said document is verified by verifying only one aggregate signature to verify entire sections of the whole document (256).

Referring to Figure 3, the method of document creation and storage 300 by the main author 107 of the document 201 is illustrated. The main author 107 creates the document and partitions the document content into sections 301. The main author 107 then signs
30 every section 302 and creates an authorization list 303, specifying which user is authorized to edit each of the sections. Initially, as mentioned above, every section is signed 302 by the main author 107. The list of section signatures will have signatures by other users when the sections are updated by co-authors 108 as discussed below. The

authorization list 202 contains all of the section names and the corresponding co-authors 108, the document name and one piece of static information about the document 201. An example of the static information is a hash of the section names list. The authorization list is signed 304 by the main author 107 to assure its integrity. This list cannot be edited by anyone except by the author. The main author 107 then sends 305 the document, the authorization list 202, the list of section signatures and the authorisation list signature 207 to the document management server 102.

As briefly discussed above, the document management server 102 then aggregates the signatures to create a document signature 306 and verifies the document signature 307. If this generates a Fail, the document management server 102 notifies the main author 107 of document rejection 308. If Success is identified, the document management server 102 verifies the authorisation list signature 309. If this Fails, the main author 107 is notified of rejection 308, but if this shows Success the document management server 102 send the document signature 205 to the main author 310.

When the main author 107 has the document signature 205, the main author 107 forms document integrity information 311 as discussed above and as discussed in more detail below with reference to Figure 7. The main author 107 then sends 312 the document integrity information 208 to the document management server 102. The document management server 102 then verifies the document integrity information 313. If this Fails, the main author 107 is notified of rejection 308. If this proves a Success the document management server 102 stores 314 the document 201, the authorisation list 202, the authorisation list signature 207, the document signature 205, the list of section signatures 203 and the document integrity information 208. The document management server 102 then notifies the main author 107 of successful document storage 315.

For reference, a protocol diagram for the document creation process as illustrated in Figure 3 is outlined in Figure 4.

Referring to Figure 5, the method of document updating 500 is illustrated. In this process, a user initially sends a retrieve request, including the user's identifier and the document name 501. The document management server 102 first verifies the document

502 and verifies the authorization list 503 to ensure the document 201 and the authorisation list 202 have not been modified. This may involve verifying the document integrity information 208 and occurs before sending the document and related data to the user. If the document Fails to be verified, the process is terminated. If the
5 authorisation list Fails to be verified, the document management server 102 sends a read-only copy of the document 201 to the user 504. If the verification of the document 502 and verification of the authorisation list 503 both indicate Success, the document management server 102 checks whether the user identifier supplied by the user is included in the authorisation list 505. If not, a read-only copy of the document is sent to
10 the user 504. If the user identifier is included in the authorisation list the document management server 102 sends an editable copy of the document 201 to the user 506.

On receipt of the document 201, the user then verifies the document 507. If this Fails, the process is terminated. If this shows Success the user updates a section of the
15 document 508. The user then signs the section that has been updated with their user identifier and a current timestamp 509 and sends the updated document with the new section signature to the document management server 510.

The server then checks the authorisation list 511 to ensure that the user is authorised to
20 make alterations to the section. If not, the document management server 102 notifies the user of unauthorised update 514. If authorisation is confirmed the document management server 102 verifies the new section signature 513. If this Fails the document management server 102 notifies the user of update rejection 512. If this shows Success the server replaces the signature of the section in the list of section
25 signatures 203 with the new section signature 515 and aggregates the signatures in the list 516. The server then verifies the new document signature 517. If this Fails the server notifies the user of update rejection 512. If this shows Success the server sends the user the new document signature 518.

30 On receipt of the new document signature, the user creates new document integrity information and sends this to the document management server 519. The document management server 102 then verifies the new document integrity information 520. If this Fails, the user is notified of update rejection 512, If this shows Success the document

management server 102 stores the document and related data 521. The document management server 102 then notifies the user of document update success 522.

For reference, a protocol diagram for the document update process as illustrated in Figure 5 is outlined in Figure 6.

Referring to Figure 7, a process of creating and verifying document integrity information is illustrated. Creation of the document integrity information 710 includes an initial step of the document management server 102 sending 711 a user the document signature 205 and the authorisation list signature 207. The user then hashes the document 712 and concatenates data 713 including the document hash 206, the document signature 205 and the authorisation list signature 207. The user then signs the string 714.

The verification process 720 includes an initial step of the document management server hashing the document 721. The server then extracts the document signature 205 and the authorisation signature 207 from storage or memory 722 and concatenates data 723 including the document hash 206, the document signature 205 and the authorisation list signature 207. The document management server 201 then inputs the document integrity information 208 and the string to the digital signature module 106 of the user 724. The digital signature module output is taken as the result 725.

Referring to Figure 8, a document verification process flow is illustrated. On the server side of the process 810 the server verifies the document integrity information 811. If this Fails the document is considered to be not authentic 812. If this shows Success the server verifies the document signature 813. Again if this Fails, the document is considered to be not authentic 812. If this shows Success the process is concluded and the documents authenticity confirmed 814. On the user side of the process 820 the user verifies the document signature 821. If verification of document signature fails, the document is considered not authentic 822 and if verification of document signature is successful, the process is concluded and the documents authenticity confirmed 823.

Referring to Figure 9, a further method for creating collaborative document is illustrated. User hashes the document (902) and concatenates the document hash, the document

signature and the authorization list signature (904). Thereafter, user signs the string (906) and sends the signature to the server (908). The server concatenates the document hash, the document signature and the authorization list signature (910). User's signature is verified on the string (912) and upon successful verification of user's signature, the string is signed (914) and user's signature is combined with server's signature (916). Subsequently, user's signature and server's signature is deleted (918) and server's verification key is combined with user's verification key (920). However, should the verification of user's signature on the string fails, the process of creating collaborative document ends.

As discussed above, in order to link the document 201 and the authorization list 202, the user who last edits the document signs a string which is a concatenation of the hash of the document 206, the document signature 205 and the authorization list signature 207. This signature is named the document integrity information 208. This way no adversary can replace the authorization list 202 with an authorization list of another document. A motivation for the adversary to do this is to gain editing authorization to a document for which he or she is not named as co-author. In addition, because of the algorithm for aggregate signature verification, it is possible for an adversary to add a section to the document undetected. So, the hash of the document 206 must be recorded and protected against replacement. A user is required to sign the defined string so that if the adversary gets control of the document management server 102 and hence the server's signing key, the adversary still would not be able to corrupt the document integrity data.

The invention describes a system and methods to provide non-repudiation of document content creation by all co-authors by having them to digitally sign the sections they updated. However, by deploying aggregate signature, verification of the document signature takes less time than verifying every section signature. Besides that, the methods are carefully designed to make any modification to the document or their related data by an adversary who gets control of the document management server can be detected.

Unless the context requires otherwise or specifically stated to the contrary, integers, steps or elements of the invention recited herein as singular integers, steps or elements

clearly encompass both singular and plural forms of the recited integers, steps or elements.

5 Throughout this specification, unless the context requires otherwise, the word
“comprise”, or variations such as “comprises” or “comprising”, will be understood to imply
the inclusion of a stated step or element or integer or group of steps or elements or
integers, but not the exclusion of any other step or element or integer or group of steps,
elements or integers. Thus, in the context of this specification, the term “comprising” is
used in an inclusive sense and thus should be understood as meaning “including
10 principally, but not necessarily solely”.

It will be appreciated that the foregoing description has been given by way of illustrative
example of the invention and that all such modifications and variations thereto as would
be apparent to persons of skill in the art are deemed to fall within the broad scope and
15 ambit of the invention as herein set forth.

CLAIMS

1. A system (100) for non-repudiable collaborative updates of document creation comprising:

5 at least one document management server (102) adapted to manage document storage (101) and having an associated pair of signing and verification keys;

 at least two clients (104) each having a unique identifier and a pair of signing and verification keys, said verification keys of said clients being

10 available to said document management server (102) and to other clients;

 at least one document management module (103) adapted to receive service requests from said clients;

 at least one aggregate signature module (105) residing in said document management server; and

15 a corresponding number of digital signature modules (106) residing in each of said clients;

 characterized in that said aggregate signature module (105) produces one aggregate signature to verify sections of the whole document; said aggregate signature module further comprises steps of:

20 signing messages using the document management server signing key;

 verifying signatures on messages given a signature, verification key and message;

 aggregating a set of signatures to produce an aggregate signature;

25 and

 verifying said aggregate signature given said aggregate signature, a set of associated verification keys and a set of associated messages.

- 30 2. A system (100) according to claim 1, wherein the corresponding number of digital signature modules (106) associated with each of said clients further having means for:
- signing messages using the respective client signing keys;

verifying signatures and messages given a signature, verification key and message; and

verifying said aggregate signature given said aggregate signature, a set of associated verification keys and a set of associated messages.

5

3. A system (100) according to claim 1, wherein interactions between said clients and said document management server (102) are conducted over an authenticated channel.

10

4. A system (100) as claimed in claim 1, wherein said document storage (101) is located on a storage server connected to said document management server (102).

15

5. A system (100) as claimed in claim 1, wherein said document management module (103) is adapted to store and extract documents from said storage server (102).

20

6. A system (100) as claimed in claim 1, wherein said document management module (103) is located in said document management server (102).

7. A system (100) as claimed in claim 1, wherein said verification keys are stored in the document management server (102) or in a separate repository that is accessible to said document management server and said clients.

25

8. A method (250) for non-repudiable updates of document; the method comprising steps of:

creating collaborative document (252);

updating collaborative document (254);

verifying document integrity (256)

30

characterized in that updating collaborative document (254) further comprises steps of:

a client sending a document extraction request with a user identifier to said document management server (501);

said document management server verifying document integrity information (501a);

said document management server verifying said document signature (502);

5 said document management server verifying said authorisation list signature (503);

said document management server checking whether said user identifier is included in said authorisation list (505);

10 if said user identifier is included in said authorisation list, said document management server sending an editable form of said document to said user together with said document signature (506);

said user verifying the document signature (507);

15 said user updating a section of said document to form an updated document (508);

said user signing the updated section of said updated document appended with said user identifier and current timestamp to form a new section signature (509);

20 said user sending the updated document and new section signature to said document management server (510);

said document management server confirming with said authorisation list that said user is authorised to update said section (511);

25 said document management server verifying said new section signature (513);

said document management server updating said list of section signatures (515) and aggregating said signatures to form a new document signature (516);

30 said document management server verifying said new document signature (517);

said document management server sending said new document signature and said authorisation list signature to said user (518);

said user hashing the updated document and signing a string containing the hash of said document, said new document signature and said authorisation list signature to form new document integrity information;

5 said user sending said document integrity information to said document management server (519);
 said document management server verifying said new document integrity information (520); and

10 said document management server storing said updated document, said authorisation list; said updated list of section signatures; said new document signature, said new document integrity information and a user identifier (521).

9. A method (300) according to claim 8, wherein creating collaborative document
15 (252) further comprising steps of:

 a user creating a document with defined sections (301);
 said user signing each of said defined sections to form a list of section
 signatures (302);
 said user creating an authorisation list and signing said authorization list
20 (303, 304);

 said user sending said document, said authorization list, said list of
 section signatures and said authorisation list signature to at least one
 document management server (305);

25 said document management server aggregating signatures in said list of
 section signatures to form a document signature (306);

 said document management server verifying said document with said
 document signature (307);

 said document management server verifying said authorisation list with
 said authorisation list signature (309);

30 said document management server sending said document signature to
 said user (310);

said user hashing said document and signing a string containing said hash of said document, said document signature and said authorisation list signature to form document integrity information (311);
said user sending said document integrity information to said document management server (312); said document management server verifying said document integrity information (313); and
said document management server storing said document, said authorisation list, said list of section signatures; said document signature, said document integrity information and a user identifier (314).

10

10. A method as claimed in claim 9 , wherein said authorisation list comprises at least the name of said document, a list of all sections of said document, a list of users authorised to update each section of said document and a static content of said document.

15

11. A method as claimed in claim 10, wherein said static content of said document is hash of said list of all sections of said document.

20

12. A further method (900) for creating collaborative document as claimed in claim 8, further comprising steps of:

hashing document (902) and concatenating said document hash, document signature and authorization list signature (904);
signing string (906) and sending signature to server (908);
concatenating said document hash, document signature and authorization list signature at server (910);
verifying user signature on said string (912);
signing said string (914) and combining user's signature and server's signature (916);
deleting user's signature and server's signature (918); and
combining server verification key and user's verification key (920).

25

30

13. A method (800) as claimed in claim 8, wherein verification of said document by said document management server comprises:

verifying said document integrity information (811); and
if verified, verifying said document signature (813); or
if not verified, stopping said method (812).

14. A method (700) as claimed in claim 8, wherein verifying said document integrity information by said document management server comprises:

creating document integrity information by:

sending document signature and authorization list signature to user (711);

hashing said document by user (712);

concatenates document hash, document signature and authorization list signature by user (713);

signing the string by user (714)

verifying said document integrity information by:

hashing said document (721);

extracting said document signature and said authorisation list signature (722);

forming a string containing the document hash, said document signature and said authorisation list signature (723);

inputting to a digital signature module associated with a client of a user the document integrity information and said formed string and a user verification key associated with a user whose user identifier is in the document integrity information (724); and

taking the output of the module as the result (725).

100

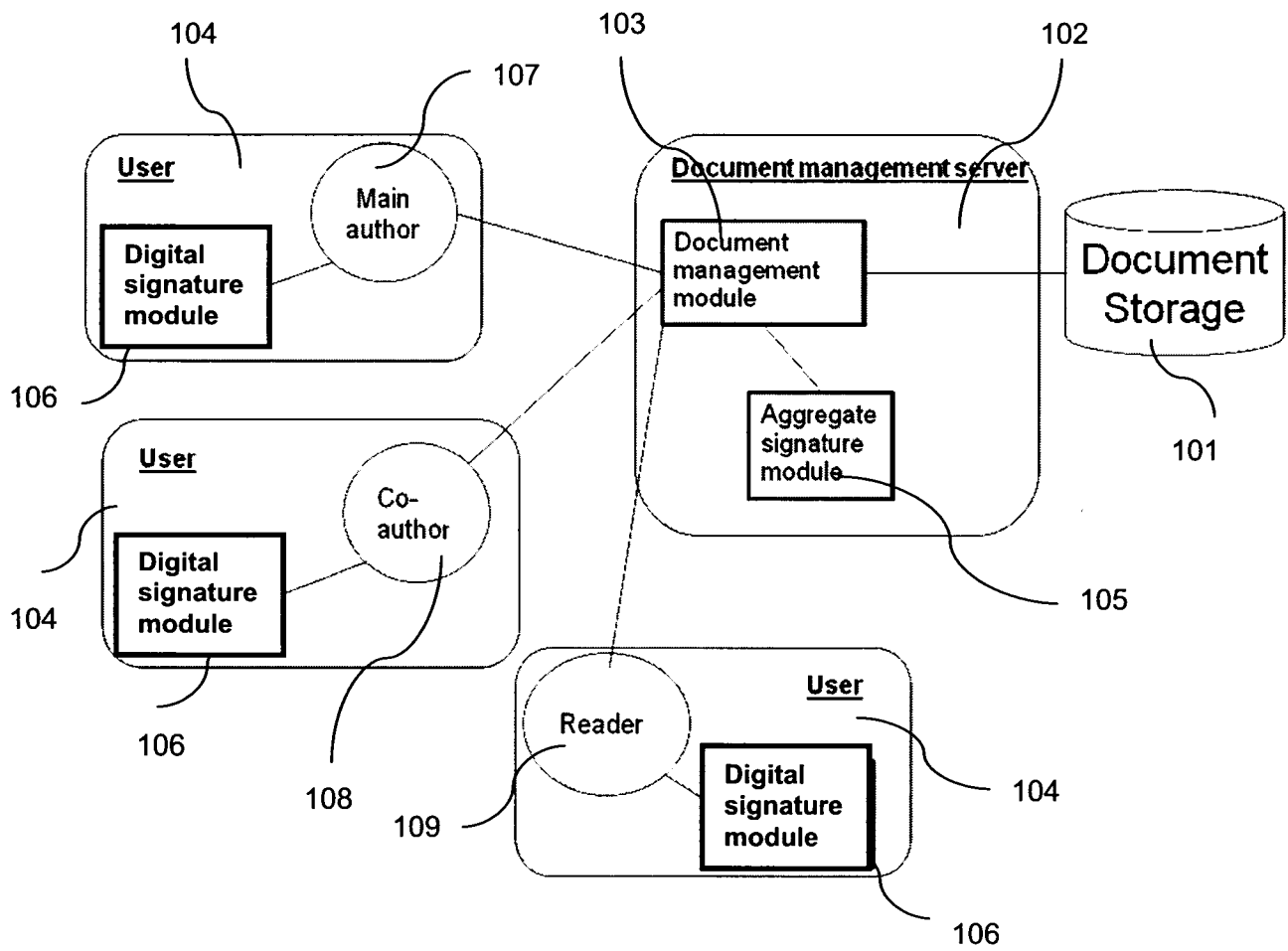


Figure 1.0

200

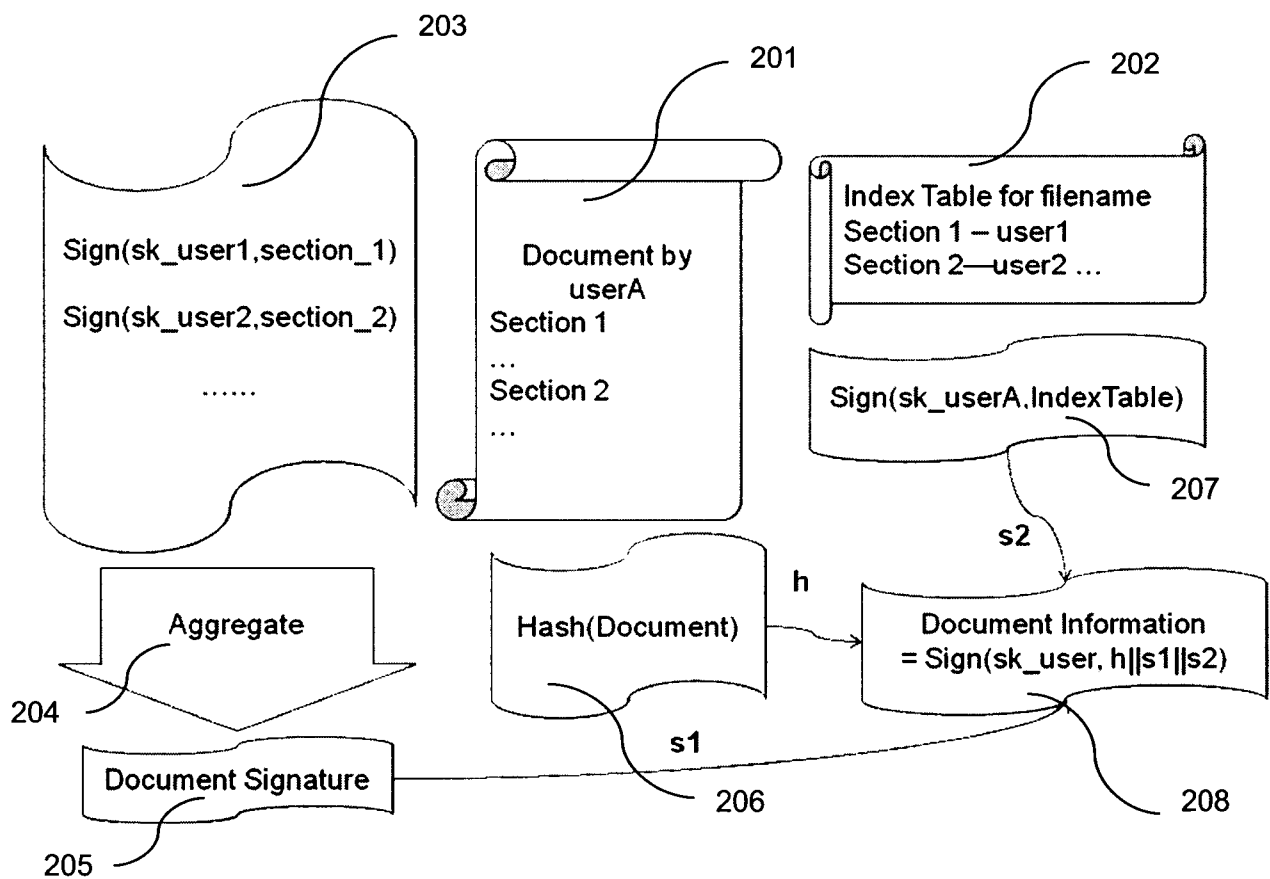


Figure 2.0

250

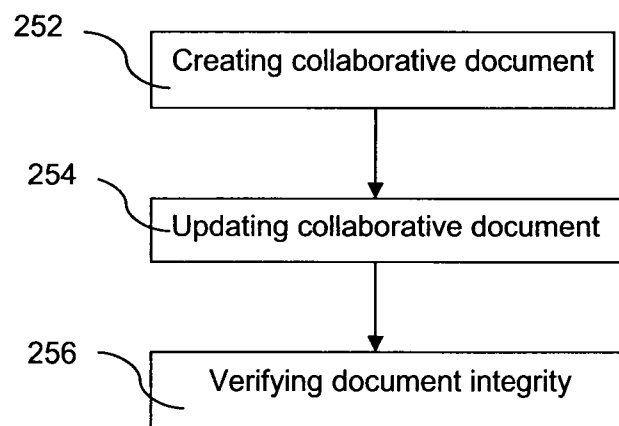


Figure 2A

300

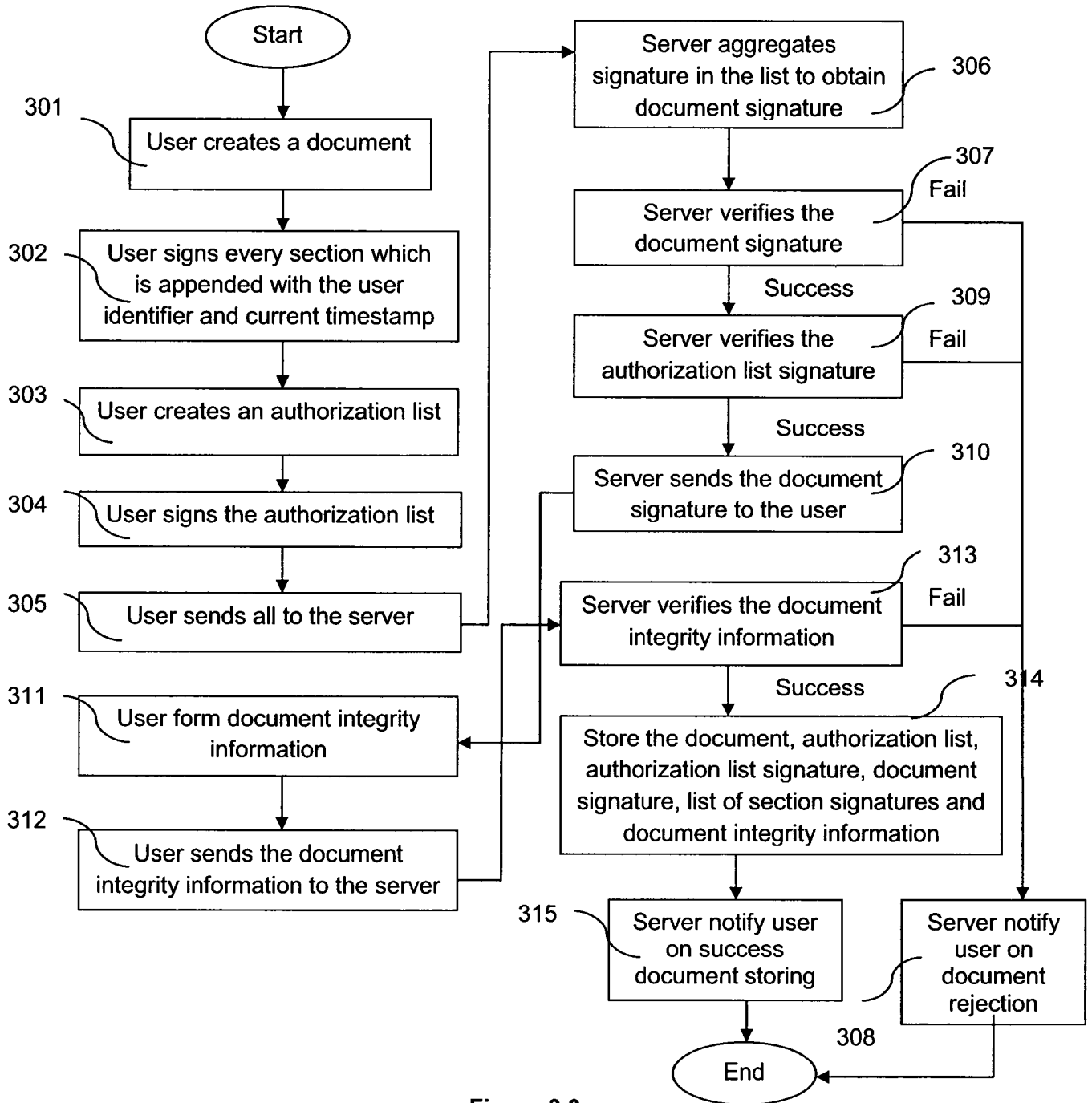


Figure 3.0

400

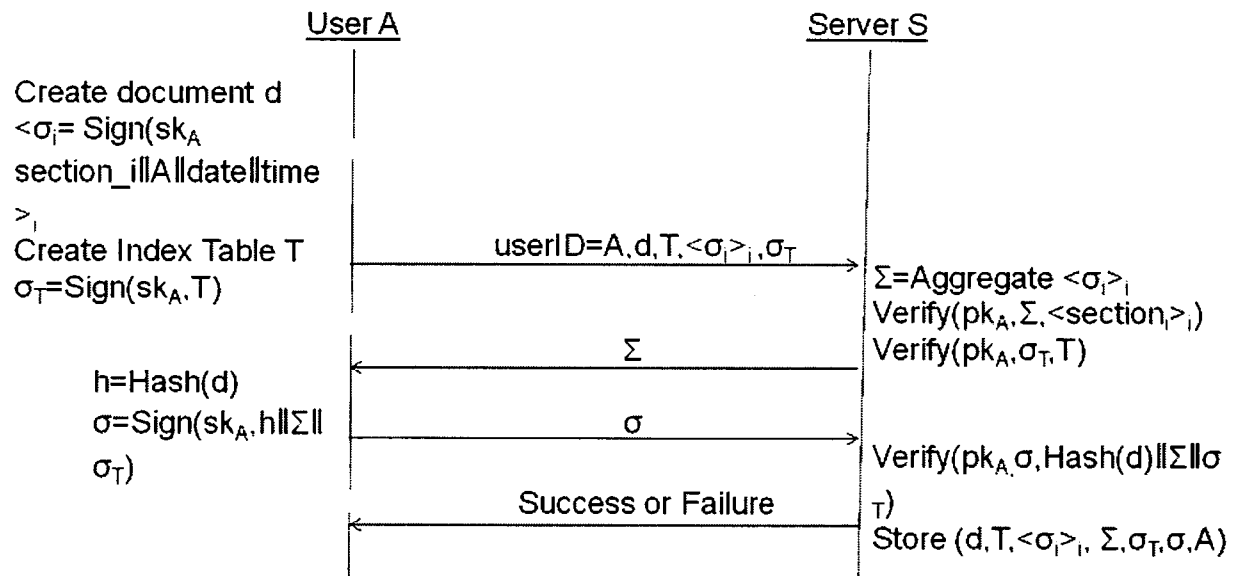
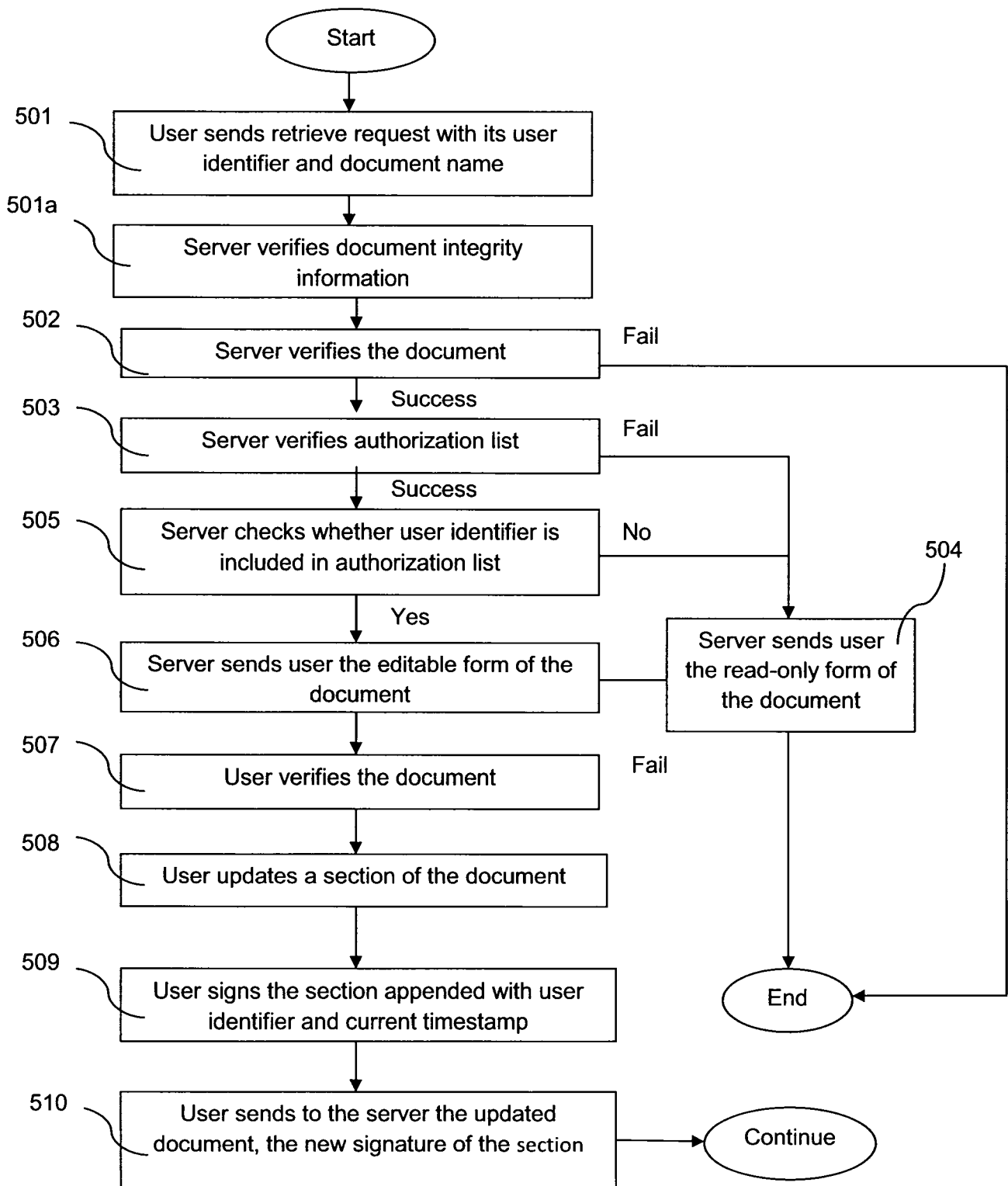


Figure 4.0

500



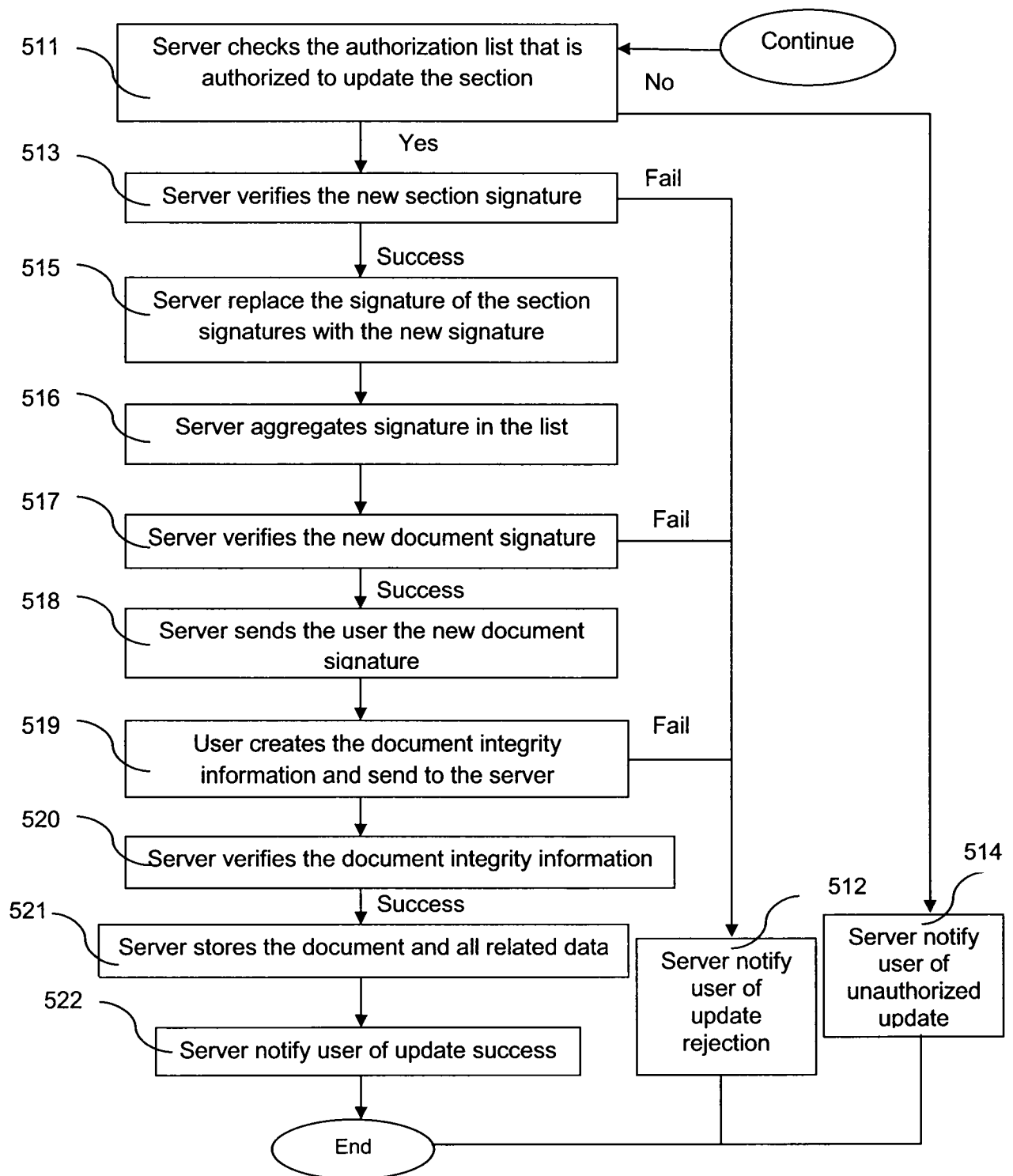


Figure 5.0

600

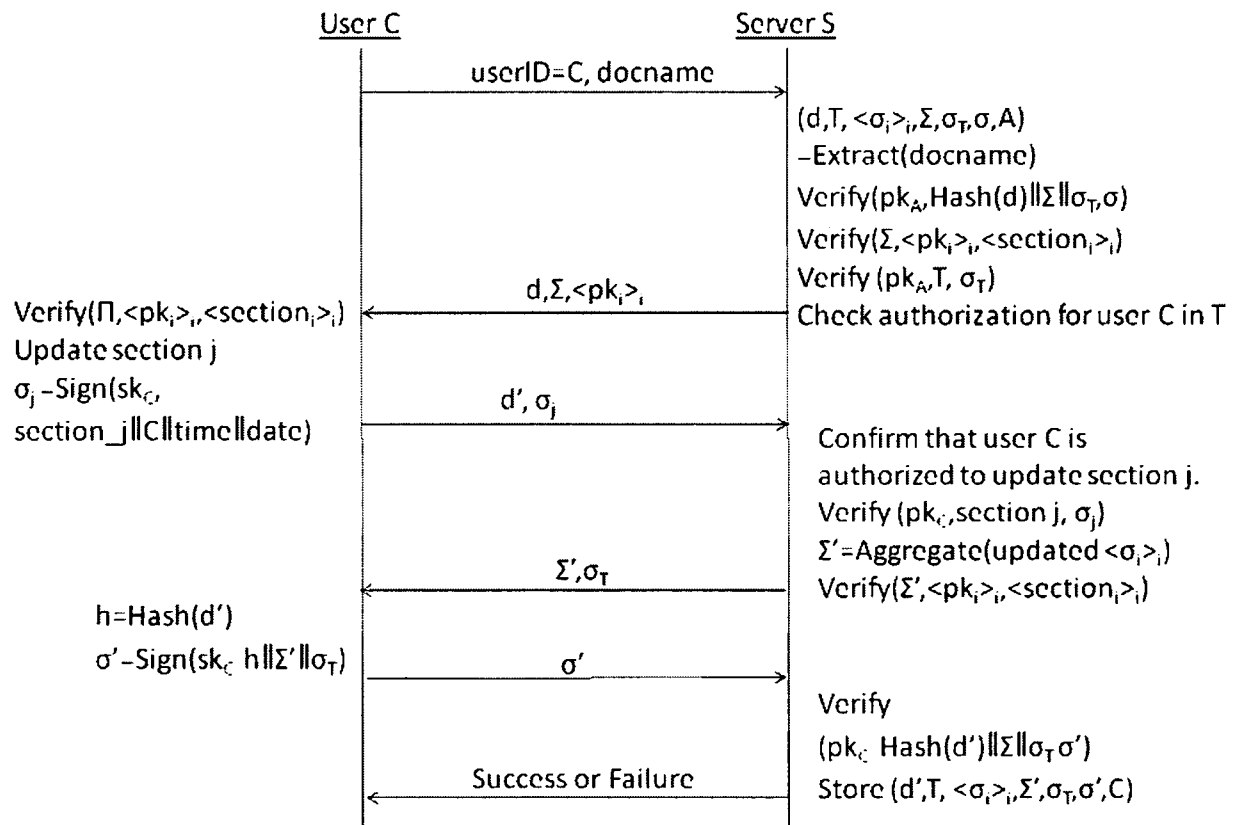


Figure 6.0

700

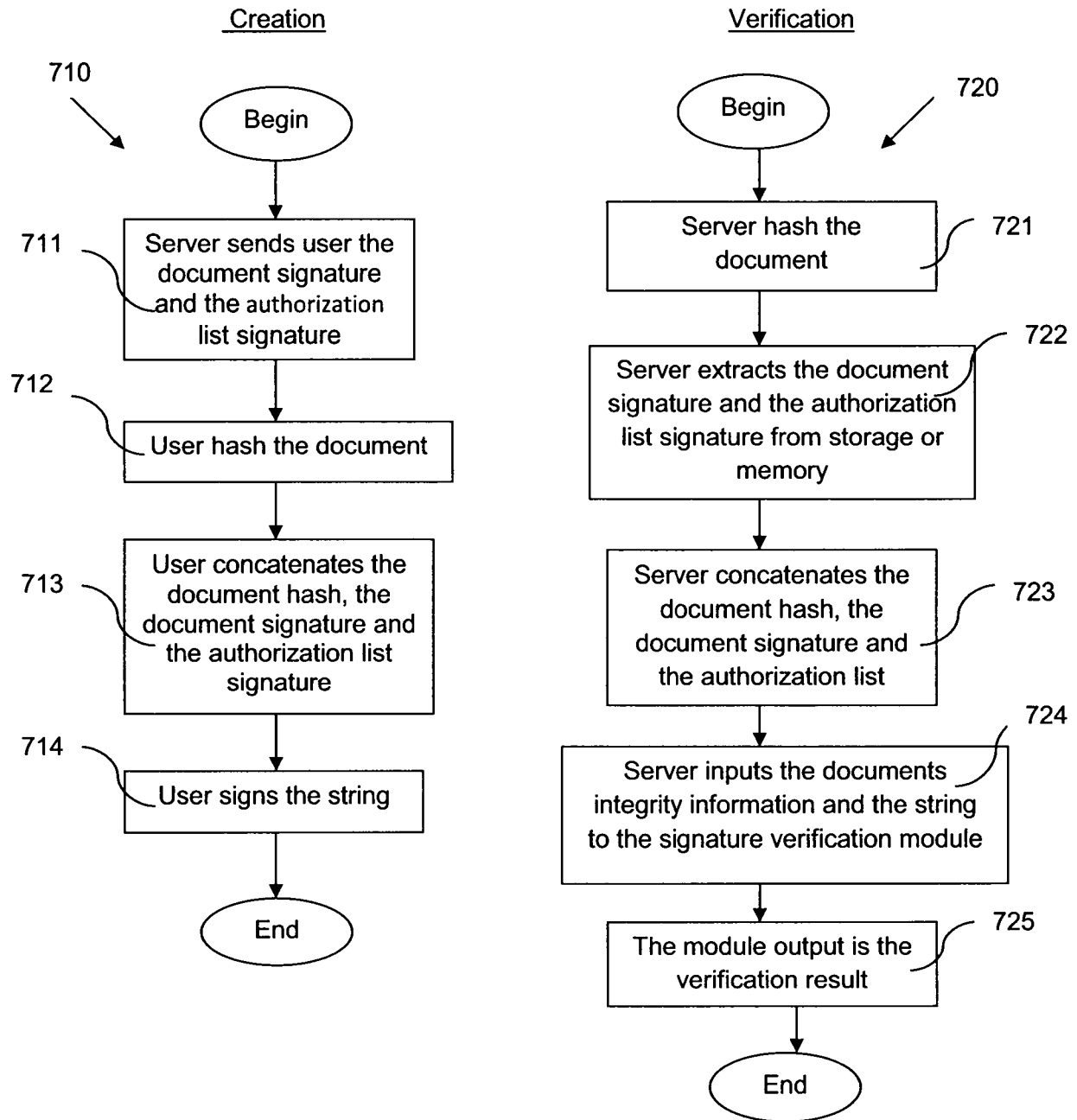


Figure 7.0

800

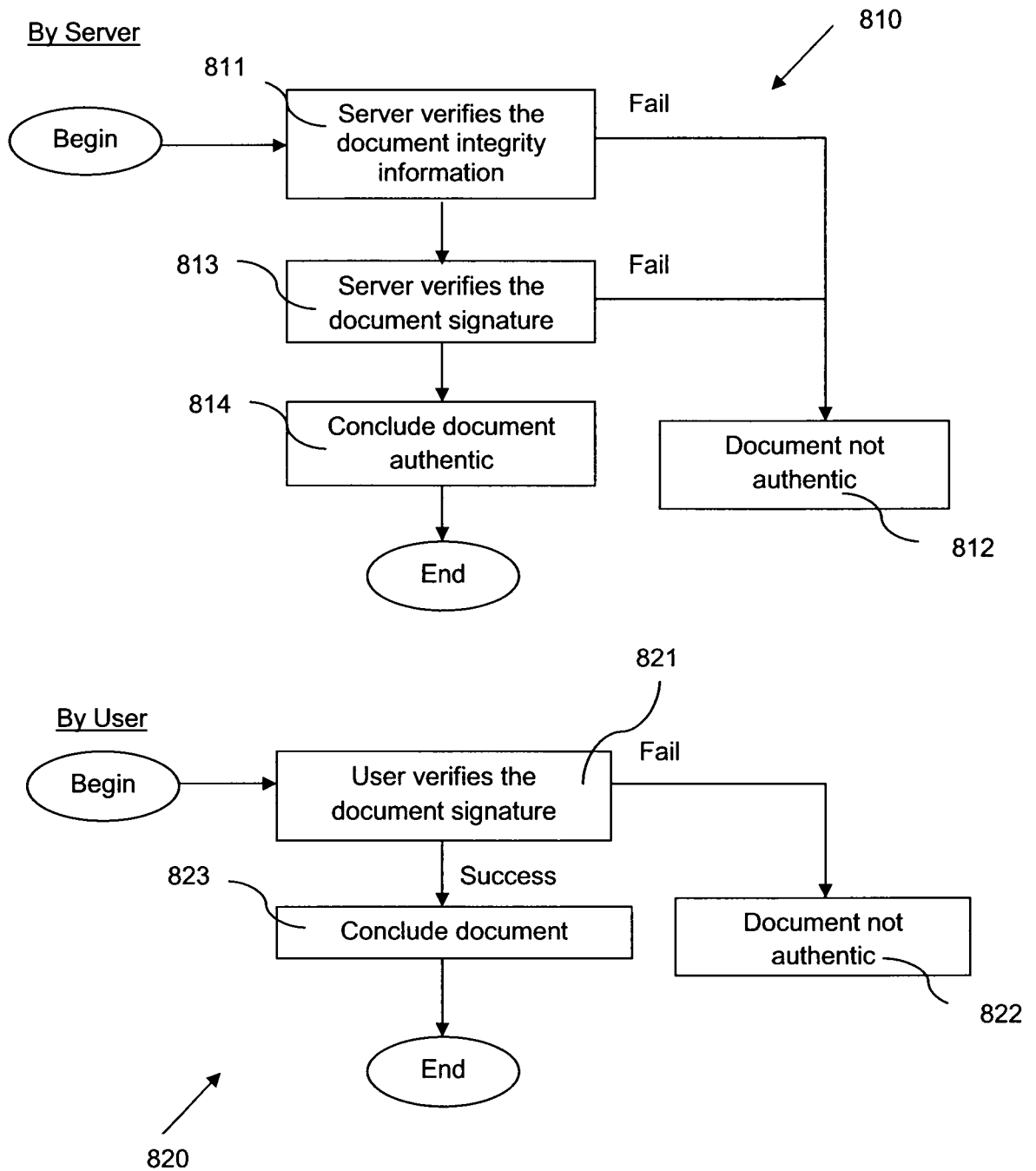


Figure 8.0

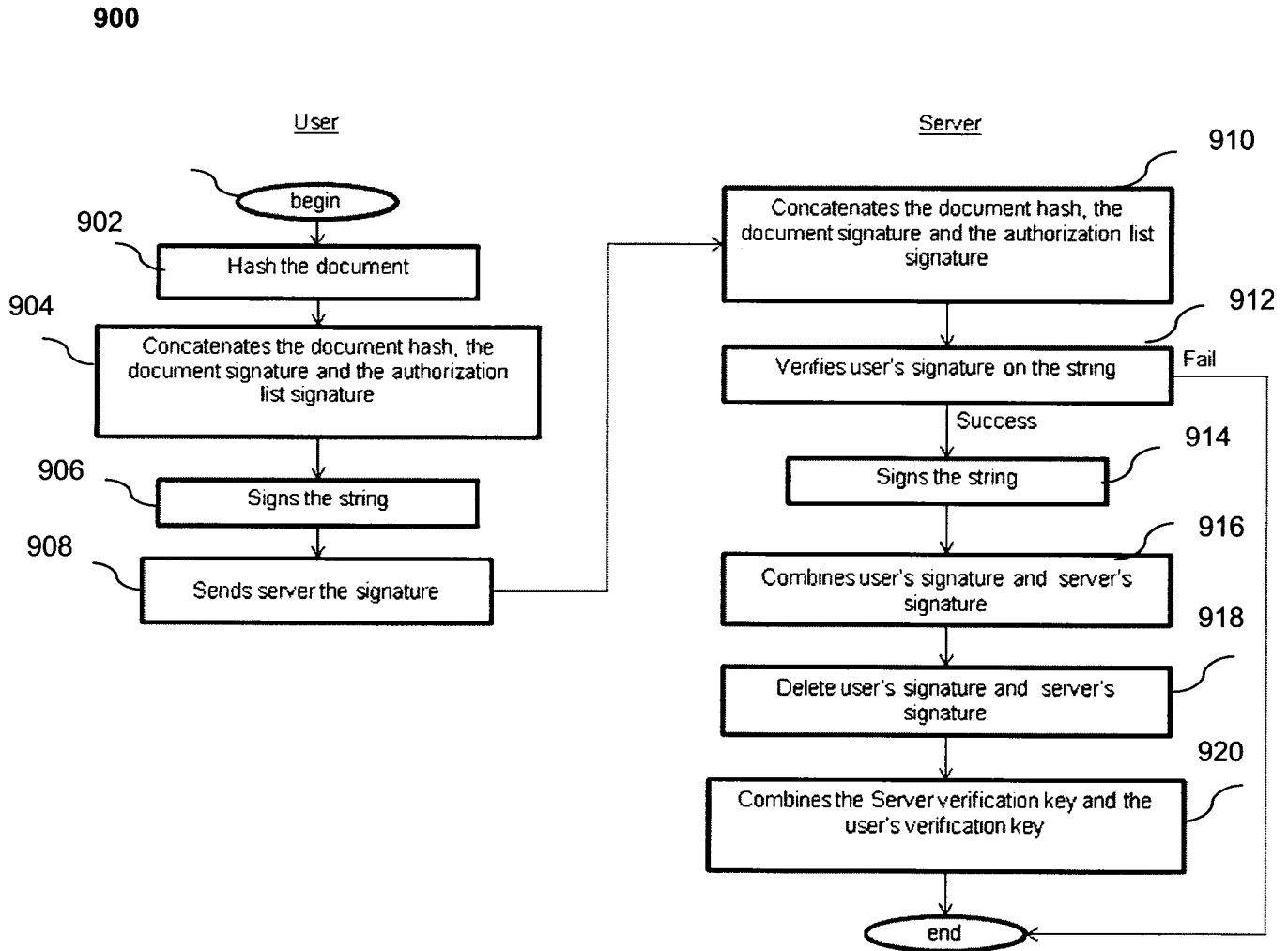


Figure 9.0

INTERNATIONAL SEARCH REPORT

International application No
PCT/MY2014/000067

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/64
ADD.

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

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

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

EP0-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2007/168672 A1 (IZU TETSUYA [JP] ET AL) 19 July 2007 (2007-07-19) paragraph [0277] - paragraph [0300]; claims 10, 13; figure 2 paragraph [0482] - paragraph [0552] -----	1-14

☐

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 another 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

23 October 2014

Date of mailing of the international search report

04/11/2014

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Savvides, George

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/MY2014/000067

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2007168672 A1	19-07-2007	CN 101004805 A	25-07-2007
		EP 1808795 A2	18-07-2007
		JP 5028884 B2	19-09-2012
		JP 2007213549 A	23-08-2007
		KR 20070076376 A	24-07-2007
		US 2007168671 A1	19-07-2007
		US 2007168672 A1	19-07-2007
