

METHOD AND SYSTEM FOR DIGITALLY SIGNING A DOCUMENT

Field of the Invention

The present invention relates to a method and system for digitally signing a document.

5

Background of the Invention

A digital signature is an important component of electronic commerce as it provides the condition of non-repudiation when an electronic contract is executed. Digital signatures are employed to affirm that the person whose signature has been applied to a document wrote or otherwise agreed to the contents of the document to which the digital signature is attached. They are thus analogues of conventional signatures.

10

However, digital signatures may provide a greater degree of security than a handwritten signature. Existing digital signatures can be used, in addition, to indicate to a recipient that the content of the document or message has not been altered either intentionally or accidentally after signing. A user can do this, in an existing approach, by creating a message digest by applying a hash function to the document. The message digest serves as a “digital fingerprint” of the document; if any part of the document is modified, the hash function returned by the altered document is different. The user then encrypts the message digest with his or her private key, and uses the encrypted message digest as the digital signature of the document.

15

20

Thus, a digital signature enables the authentication of digital documents, assuring the recipient of a digital document of both the identity of the sender and the integrity of the content. Digital signatures are therefore useful for e-commerce, as they made it difficult to repudiate a contract signed with such a digital signature.

25

In spite of the benefits of digital signatures, however, they are not widely used, mainly—it appears—owing to difficulty of use. In addition, there are costs associated with digital signatures for both users and recipients. Also, existing electronic signatures are unable to create reliable e-contracts because they do not provide adequate and convenient non-repudiation.

30

For example, one existing approach is disclosed in US Publication No. US 2005/0216742. According to the disclosed technique, each of an organization’s representatives is provided with a private/public key issued from a certified public key service provider. Consumers sign the e-contracts using electronic signatures but the

35

representatives counter-sign with his/her private key in order to create a secure electronic record.

5 However, the resulting e-contract is still insufficiently robust for some purposes. For example, the disclosed approach does not address the scenario of the signed e-contract being discarded by the organization immediately after signing.

Summary of the Invention

10 It is an object of the present invention to provide method and system for digitally signing a document that goes some way to overcoming the above mentioned disadvantages or which will at least provide the public with a useful choice.

Accordingly in a first broad aspect of the present invention, there is provided a system for digitally signing a document (such as an e-contract), comprising:

15 a digital signature controller arranged to apply one or more digital signatures to the document; and

a witnessing server in data communication with the digital signature controller; wherein the system is adapted to digitally sign a document with the digital signature controller and forward either the document once digitally signed or a hash value derived from the document once digitally signed to the witnessing server, and the witnessing server is arranged to apply a further digital signature to the document or the hash of the document and then to output the document or the hash value (that is, with applied further digital signature).

25 The hash value may be derived from the document in any suitable manner.

Thus, the system and method of this invention will find diverse application, such as in facilitating the creation, amendment or closure/termination of bank and other financial institution accounts (including loan accounts), insurance policies, contracts for services, etc., as well as—for example—in facilitating the issuance of eCheques, money orders, overdrafts and other financial instruments.

35 The system may include a device to facilitate electronically signing the document (such as with an electronic stylus and tablet, a finger print scanner or retinal scanner), typically before applying the digital signature to the document.

In another embodiment, the system is adapted to electronically sign the document with

the digital signature.

In embodiments in which the system is adapted to forward the hash value to the witnessing server, the hash value may be encrypted or unencrypted. If encrypted, the
5 hash value may comprise the digital signature.

In a certain embodiment, the system is adapted to receive user input comprising at least one identifying characteristic of an intended signatory, and to apply an electronic or digital signature to the document derived from the input, such as with the digital
10 signature controller.

In one embodiment, the system is arranged to:
receive data indicative of the document;
render the data as a representation of the document on a display;
15 request input of at least one identifying characteristic of an intended signatory;
capture the input corresponding to the at least one identifying characteristic;
modify the document according to the input (and hence electronically sign the document).

20 Thus, the system can capture and apply an electronic signature to the document.

The input may comprise one or more signatures or biometric data (such as retinal or fingerprint scan data).

25 The system may be arranged to modify the document according to the input by adding the input or data derived therefrom to the document.

In another particular embodiment, the digital signature controller is arranged to apply the one or more digital signatures to the document by outputting the document and the
30 one or more digital signatures to a single file.

In a further embodiment, the digital signature controller is arranged to output the document and the one or more digital signatures as separate files.

35 In a certain embodiment, the digital signature controller is arranged to derive the one or more digital signatures by a method comprising forming a hash value from the document.

In another embodiment, the digital signature controller comprises:

- a processor;
- a memory;
- 5 a display responsive to the processor.

In another embodiment, the witnessing server is arranged to timestamp the document or the hash value before applying the further digital signature to the document or the hash value.

10

In a certain embodiment, the witnessing server is arranged to apply a digital watermark or confidence mark to the document or the hash value before applying the further digital signature to the document or the hash value.

15 Thus, the witnessing server can provide authentication in any suitable way.

In a particular embodiment, the witnessing server applies the further digital signature to the document or to the hash value, by producing a hash either of the document and a timestamp or of the hash value and a timestamp, and digitally signing the hash with a private key of the witnessing server.

20

In another embodiment, the witnessing server is arranged to output the document or the hash value after applying the further digital signature to a data store.

25 In another embodiment, the witnessing server is arranged to forward the document or the hash value after applying the further digital signature to a specified recipient (which may be the party—or computing device—that created or originally digitally signed the document).

30 Accordingly in a second broad aspect of the present invention, there is provided a method of digitally signing a document, comprising:

- applying one or more digital signatures to the document;
- forwarding either the document once digitally signed or a hash value derived from the document once digitally signed to a remote server (referred to as a
- 35 'witnessing server' in some embodiments);
- applying a further digital signature to the document or the hash of the document with the remote server; and

outputting the document or the hash value.

5 The method may include electronically signing the document (such as with an electronic stylus and tablet, a finger print scanner or retinal scanner) before applying the digital signature to the document.

10 In another embodiment, method includes electronically signing the document with the digital signature, such that the document is electronically and digitally signed effectively simultaneously.

10 In embodiments in which the method includes forwarding the hash value to the remote server, the hash value may be encrypted or unencrypted. If encrypted, the hash value may comprise the digital signature.

15 In a particular embodiment, the method includes receiving user input comprising at least one identifying characteristic of an intended signatory, and applying an electronic or digital signature to the document derived from the user input.

20 In one embodiment, the method comprises:
displaying the document on a display;
requesting input of at least one identifying characteristic of an intended signatory;
capturing the input corresponding to the at least one identifying characteristic;
and
25 modifying the document according to the input (and hence electronically sign the document).

The input may be, for example, a signature (or signatures) or biometric data.

30 The method may include modifying the document according to the input by adding the input or data derived therefrom to the document.

35 In another embodiment, the method includes applying the one or more digital signatures to the document by outputting the document and the one or more digital signatures to a single file.

In still another embodiment, the method includes deriving the one or more digital

signatures by forming a hash value from the document.

5 In yet another embodiment, the method includes the remote server timestamping the document or hash value before applying the further digital signature to the document or hash value.

10 In one embodiment, the method includes the remote server applying a digital watermark or confidence mark to the document or the hash value before applying the further digital signature to the document or the hash value.

15 In a particular embodiment, the method includes the remote server applying the further digital signature to the document or to the hash value, by producing a hash either of the document and a timestamp or of the hash value and a timestamp, and digitally signing the hash with a private key of the remote server.

20 In a certain embodiment, the method includes the remote server outputting the document or hash value after applying the further digital signature to a data store.

In another embodiment, the method includes the remote server forwarding the document or hash value after applying the further digital signature to a specified recipient.

25 Accordingly in a third broad aspect of the present invention, there is provided a digital witnessing system, comprising:

a witnessing server in data communication with a remote computing device;
wherein the server is adapted to receive electronically either a digitally signed document or a hash value derived from the digitally signed document from the device, to apply a further digital signature to the document or hash value and to output the document or hash value.

30 The witnessing server may be adapted to timestamp the digitally signed document or hash value before applying the further digital signature.

35 In one embodiment, the witnessing server is arranged to apply a digital watermark or confidence mark to the document or the hash value before applying the further digital signature.

In embodiments in which the witnessing server receives the hash value, the hash value may be encrypted or unencrypted. If encrypted, the hash value may comprise a digital signature used to sign the digitally signed document.

- 5 It should be noted that any of the various features of each of the above aspects of the invention, and of the various features of the embodiments described below, can be combined as suitable and desired.

Brief Description of the Drawings

- 10 In order that the invention may be more clearly ascertained, embodiments will now be described, by way of example, with reference to the accompanying drawing, in which:

FIG. 1 is a schematic diagram of a system for applying a digital signature to a document according to an embodiment of the present invention;

FIG. 2 is a schematic diagram of the user computer of the system of FIG. 1;

- 15 FIG. 3 is a schematic diagram of the digital signature controller of the user computer of FIG. 2;

FIG. 4 is a schematic diagram of the witnessing server of the system of FIG. 1; and

- 20 FIGS. 5A and 5B depict a flow diagram of a method implemented by the system of FIG. 1 according to an embodiment of the present invention.

Detailed Description of the Invention

- FIG. 1 is a schematic diagram of a system 10 for applying a digital signature to a document according to an embodiment of the present invention (shown with a recipient computer, that is, the computer of the intended recipient of the document). System 10 includes a user computer 12, a witnessing server 14 and a telecommunications network 16. Telecommunications network 16 is also used to transmit the document, once digitally signed, to a recipient computer 18.

- 30 User computer 12 may assume many acceptable forms, including a laptop or desktop computer, a portable communications device (such as a smart phone or PDA) or a tablet computer, and in this embodiment is in the form of a laptop computer. Telecommunications network 16 may be a public or private network (or, indeed, virtual private network), such as an intranet or the internet; in this embodiment
- 35 telecommunications network 16 comprises the internet.

FIG. 2 is a schematic diagram of user computer 12, which includes a digital signature

controller 20 comprising a processor 22, memory 24, a network card 26 (for facilitating communication with telecommunications network 16) and an input/output (I/O) interface 28 for communicating with, for example, peripheral devices of user computer 12. Herein the term “processor” is used to refer generically to any device that can
5 process instructions embodying the method of this embodiment, and may include a microprocessor, microcontroller, programmable logic device or other computational device, a general purpose computer (e.g. a PC) or a server. Typically, the instructions are stored as program code in memory 24 but can also be hardwired.

10 User computer 12 also includes a data store 30, which may comprise a hard drive or solid state storage and which communicates with processor 22 via I/O interface 28. User computer 12 also includes, in data communication with digital signature controller 20, a user interface 32 comprising a display 34, a touch screen 36, a printer/scanner 38 and a keyboard 40. Touch screen 36 is adapted, in this embodiment, to be used to
15 control user computer 12 (through user interaction with control icons displayed by processor 22 to touch screen 36). However, user interface 32 also includes a stylus that can be used by a user to ‘write’ on touch screen 36 and thereby enter information (including his or her signature). Indeed, in some embodiments, touch screen 36 is provided as a pen tablet that is in wireless communication with digital signature
20 controller 20. User computer also includes a biometric reader 42, which may be adapted to capture any desired biometric information, such as an iris scan or one or more fingerprints.

Thus, both touch screen 36 and biometric reader 42 may be used by a user to enter an
25 identifying characteristic (such as a signature, iris scan or fingerprint), which is to be used in electronically signing the document, typically by a customer (as a customer is less likely to be equipped to execute the document with a digital signature than would be a vendor such as a financial institution). In some embodiments, however, system 10 is adapted to accommodate the application of a digital signature by a customer
30 (possibly in addition to the application of a electronic signature). In such embodiments, system 10 receives the (for example) customer’s digital key, and digital signer 50 creates a digital signature using PKI (Public Key Infrastructure) and/or an electronic signature, and applies it to the document.

35 FIG. 3 is a further schematic view of user interface 32 and digital signature controller 20 of FIG. 2, with more detail shown in digital signature controller 20. Referring to FIG 3, processor 22 of digital signature controller 20 includes a display controller 42, a

document render in the form of form renderer 44, an input capturer 46 and a form updater 48. Digital signature controller 20 controls the view that is displayed on display 34 and touch screen 36; form renderer 44 controls the rendering to display 34 of a form stored as a form template in memory 24; input capturer 46 captures user data entered
5 into user interface 32 (whether via display 34, printer/scanner 38, touch screen 36 otherwise); form updater 48 adds to a rendered form user data captured by input capturer 46. Digital signer 50 creates a digital signature using PKI (Public Key Infrastructure) and applies it to the document.

10 In addition, memory 24 includes form data 52, comprising template data 54 and user data 56; the latter includes—once entered by a user or users—an electronic signature(s) 57. Template data 52 comprises the data (in, for example, HTML, Java (trade mark) script or MS Word (trade mark), Adobe PDF (trade mark), XML (trade mark) or Open Document (trade mark) format) that, when rendered by form renderer
15 44 to display 34, constitutes an uncompleted form. User data 56 is the data entered by the user to complete the form, as captured by input capturer 46 (such as the user's personal details). Electronic signature 57 is the signature (or data indicative thereof) entered by the user to electronically sign the form; the signature may be entered by the user in any suitable manner, such as by signing touch screen 36, especially when in
20 the form of a pen tablet, or providing biometric data with biometric reader 42.

FIG. 4 is a further schematic view of witnessing server 14. Witnessing server 14 is adapted to receive documents from user computer 12 (and indeed from other user computers [not shown] also connected to telecommunications network 16) to which a
25 digital signature has been applied. Witnessing server 14 includes a processor 60 that comprises a clock 62, a timestamp 64 and a digital signer 66. Witnessing server 14 also has a memory 68 that includes a private key 70 (for use, as described below, in digitally signing documents).

30 The operation of system 10 will now be described in detail. In broad summary, however, system 10 facilitates the creation or capture of an electronic document, such as a form. This may be done either by creating the document, such as by using a word processor, by scanning a paper document and saving the scanned copy in electronic form, or receiving the form from a remote location. The parties who are to execute the
35 document check that the contents of the electronic version are as desired, then—in this embodiment—execute the document by applying their signatures to touch screen 36. System 10 captures the signatures, converts them into electronic form, and applies the

electronic signatures to the electronic document. It will be noted that one or more parties may be required to execute the document. These parties may include one or more witnesses. The state of the document at the time the electronic signature of the last party to sign (such as a witness) is known so any subsequent changes to the document result in an invalid hash.

One or more officiating parties or representatives of the signatories (including, in this embodiment, the operator of user computer 12) have digital keys 58, and user computer 12 has software and hardware (in the form of Digital signer 50) to digitally sign the document with such key(s). These digital keys 58 are obtained and entered by known techniques. As a consequence, one or more digital signatures, corresponding to these keys, can be generated and applied to the document.

The method implemented by system 10 according to this embodiment is shown as a flow diagram 80 in FIGS. 5A and 5B. At step 82, the electronic document is retrieved in template form (as template data 54) from memory 24, and rendered—at step 84—by form renderer 44 to display 34. At step 86, the party or parties who must enter information into the document enter that information (or edit it if some input fields in the document have been pre-populated) using user interface 32 (such as by typing in information with keyboard 40); this information is captured by input capturer 46 in real-time, and the document is—likewise—updated in real-time by form updater 48.

At step 88, the document—now completed—is saved to data store 30 as a single file, and—at step 90—displayed on display 34 for review by the intended signatories. At step 92, the intended signatories are presented with on-screen buttons “Accept” or “Back”, which they activate respectively according to whether they accept that the document has been completed correctly or requires amendment.

If, after step 92, one or more intended signatories activates “Back”, processing returns to step 86. Otherwise, if all intended signatories have agreed to the document by activating “Accept”, processing continues at step 94 where the intended signatories sign on touch screen 36 using their usual signatures. The stylus strokes constituting the signatures are converted into digital form 96 by touch screen 36 then captured 98 by input capturer 46; at step 100 these electronic signatures are added to the document by form updater 48.

Although user computer 12 can capture electronic signatures with touch screen 36,

some other physical indicator of agreement the system can alternatively be used to electronically sign the document, such as a finger- or thumbprint or a retina scan by biometric reader 42.

5 Furthermore, as discussed above, this step may—in alternative embodiments—be replaced or augmented by the generation and application of digital signatures by those parties that in this embodiment apply an electronic signature; in such embodiments, therefore, all parties digitally sign the document.

10 In some embodiments, the signatures are added to the document so as to appear in a specific part of the document (such as a signature panel). According to the nature of the document, the signature or signatures may be added to every page of the electronic document, if the document is multi-paged.

15 At step 102, the document—to which the electronic signature(s) have now been added—is digitally signed by digital signer 50, comprising:

i) A hash-value derived from the electronic document (termed the ‘message digest’) is calculating by applying a cryptographic hashing algorithm (such as MD2, MD4, MD5 or SHA1); the hash-value is a sequence of bits, usually with a fixed length,
20 derived in one of many possible manners—as are known in the art—from the document. In this embodiment, a mathematical transformation is applied to the document that produces a different message digest if even a single bit of input is changed.

ii) the message digest is encrypted with a private digital key of the signatories
25 (or, at a minimum as in this embodiment, with the private digital key 58 of the officiating party), thereby producing an encrypted hash-value, that is, the digital signature 59 (which is stored to memory 24). For this purpose, digital signer 50 includes an encrypting algorithm (e.g. RSA, DSA or ECDSA) for calculating digital signatures from the message digest.

30 iii) the computed digital signature 59 and the document are saved by digital signer 50 to memory store 30 as a single file (though in other embodiments, the computed digital signature 59 and the document are saved by digital signer 50 to memory store 30 in separate files, a digital signature file and a document file, respectively).

35

At step 104, the digitally signed document is forwarded via telecommunications

network 16 to witnessing server 14 which, at step 106, applies a timestamp (derived from clock 62) to the document using timestamp 64. At step 108, digital signer 66 employs private key 70 (stored in memory 68 of witnessing server 14) to generate a further digital signature. In this embodiment, this further digital signature is formed by
5 digital signer 66 in a manner similar to that implemented by digital signer 50 of user computer 12, by forming a hash-value derived from the electronic document and, optionally from the timestamp, and encrypting the hash-value with private key 70.

At step 110, the document is signed, by outputting the document and the further digital
10 signature suitably associated. According to the present embodiment, this association is effected by outputting the document and digital signature in a single file (or 'container').

At step 112, witnessing server 14 outputs the document—now digitally signed and
15 witnessed in a single file—either by returning the document, forwarding it to some other intended recipient or location, or saving the document to a secure data store 72, or a combination of these. Witnessing server 14 may comprise secure data store 72.

In an alternative embodiment, the document is not sent to witnessing server 14.
20 Instead, at step 104' a hash of the document is forwarded via telecommunications network 16 to witnessing server 14, and at step 106' witnessing server 14 applies the timestamp to the hash of the document. At step 108', digital signer 66 employs private key 70 (stored in memory 68 of witnessing server 14) to generate a further digital signature (cf. step 108), and at step 110' digital signer 66 signs the hash of the
25 document with the further digital signature. In this embodiment, the further digital signature can be generated from the hash of the document or from the hash of the document and the timestamp. At step 112', witnessing server 14 outputs the hash of the document—now digitally signed and witnessed in a single file—either by returning the hash of the document, forwarding it to some other intended recipient or location, or
30 saving the document to a secure data store 72, or a combination of these. As mentioned above, witnessing server 14 may comprise secure data store 72.

This embodiment should also reduce computing overhead, as less data need be
35 manipulated by witnessing server 14 and less data need be transmitted between user computer 12 and witnessing server 14.

Processing, in each of these embodiments, then ends.

Witnessing server 14 may thus be said to provide 'straight-through processing.' Its output may be regarded as a container that includes the date-time information, the secure electronic document or hash thereof (according to embodiment) and the digital signature of a third party (i.e. witnessing server 14).

To those skilled in the art to which the invention relates, many changes in construction and widely differing embodiments and applications of the invention will suggest themselves without departing from the scope of the invention as defined in the appended claims. The disclosures and the descriptions herein are purely illustrative and are not intended to be in any sense limiting.

In the claims that follow and in the preceding description of the invention, except where the context requires otherwise owing to express language or necessary implication, the word "comprise" or variations such as "comprises" or "comprising" is used in an inclusive sense, that is, to specify the presence of the stated features but not to preclude the presence or addition of further features in various embodiments of the invention.

Further, any reference herein to prior art is not intended to imply that such prior art forms or formed a part of the common general knowledge in any country.

CLAIMS:

1. A system for digitally signing a document, comprising:
 - a digital signature controller arranged to apply one or more digital signatures to
 - 5 the document; and
 - a witnessing server in data communication with the digital signature controller;
 - wherein the system is adapted to digitally sign a document with the digital
 - signature controller and forward either the document once digitally signed or a hash
 - value derived from the document once digitally signed to the witnessing server, and the
 - 10 witnessing server is arranged to apply a further digital signature to the document or the
 - hash of the document and then to output the document or the hash value.
2. A system as claimed in claim 1, wherein the system is adapted to forward the hash
- value to the witnessing server, and the hash value is encrypted.
- 15 3. A system as claimed in claim 2, wherein the hash value comprises the digital
- signature.
4. A system as claimed in claim 1, wherein the system is adapted to receive user input
- 20 comprising at least one identifying characteristic of an intended signatory, and to apply
- an electronic or digital signature to said document derived from said input.
5. A system as claimed in claim 1, wherein said system is arranged to:
 - receive data indicative of said document;
 - 25 render said data as a representation of said document on a display;
 - request input of at least one identifying characteristic of an intended signatory;
 - capture said input corresponding to said at least one identifying characteristic;
 - modify said document according to said input.
- 30 6. A system as claimed in claim 5, wherein said input is a signature or biometric data.
7. A system as claimed in claim 5, wherein said system is arranged to modify said
- document according to said input by adding said input or data derived therefrom to
- said document.
- 35 8. A system as claimed in claim 1, wherein said digital signature controller is arranged
- to apply said one or more digital signatures to said document by outputting said

document and said one or more digital signatures to a single file.

9. A system as claimed in claim 1, wherein said digital signature controller is arranged to output said document and said one or more digital signatures as separate files.

5

10. A system as claimed in claim 1, wherein said digital signature controller is arranged to derive said one or more digital signatures by a method comprising forming a hash value from said document.

10 11. A system as claimed in claim 1, wherein said digital signature controller comprises:

- a processor;
- a memory;
- a display responsive to said processor.

15

12. A system as claimed in claim 1, wherein said witnessing server is arranged to timestamp said document or the hash value before applying said further digital signature to said document or the hash value.

20 13. A system as claimed in claim 1, wherein said witnessing server is arranged to apply a digital watermark or confidence mark to said document or the hash value before applying said further digital signature to said document or the hash value.

25 14. A system as claimed in claim 1, wherein the witnessing server applies the further digital signature to the document or to the hash value, by producing a hash either of the document and a timestamp or of the hash value and a timestamp, and digitally signing the hash with a private key of the witnessing server.

30 15. A system as claimed in claim 1, wherein the witnessing server is arranged to output the document or the hash value after applying the further digital signature to a data store.

35 16. A system as claimed in claim 1, wherein the witnessing server is arranged to forward the document or the hash value after applying the further digital signature to a specified recipient.

17. A method of digitally signing a document, comprising:

applying one or more digital signatures to the document;
forwarding either the document once digitally signed or a hash value derived
from the document once digitally signed to a remote server;
applying a further digital signature to the document or the hash of the document
5 with the remote server; and
outputting the document or the hash value.

18. A method as claimed in claim 17, including electronically signing said document
before applying said digital signature to said document.

10

19. A method as claimed in claim 17, including forwarding the hash value to the
remote server, wherein the hash value is encrypted.

20. A method as claimed in claim 18, wherein the hash value comprises the digital
signature.

15

21. A method as claimed in claim 17, including receiving user input comprising at least
one identifying characteristic of an intended signatory, and applying an electronic or
digital signature to said document derived from said user input.

20

22. A method as claimed in claim 17, comprising:
displaying said document on a display;
requesting input of at least one identifying characteristic of an intended
signatory;
25 capturing said input corresponding to said at least one identifying characteristic;
modifying said document according to said input.

23. A method as claimed in claim 22, wherein said input is a signature or biometric
data.

30

24. A method as claimed in claim 22, including modifying said document according to
said input by adding said input or data derived therefrom to said document.

25. A method as claimed in claim 17, including applying said one or more digital
signatures to said document by outputting said document and said one or more digital
signatures to a single file.

35

26. A method as claimed in claim 17, including deriving said one or more digital signatures by a method that comprises forming a hash value from said document.

5 27. A method as claimed in claim 17, including the remote server timestamping the document or hash value before applying the further digital signature to the document or hash value.

10 28. A method as claimed in claim 17, including the remote server applying a digital watermark or confidence mark to said document or the hash value before applying said further digital signature to said document or the hash value.

15 29. A method as claimed in claim 17, including the remote server applying the further digital signature to the document or to the hash value, by producing a hash either of the document and a timestamp or of the hash value and a timestamp, and digitally signing the hash with a private key of the remote server.

30. A method as claimed in claim 17, including the remote server outputting the document or hash value after applying the further digital signature to a data store.

20 31. A method as claimed in claim 17, including the remote server forwarding the document or hash value after applying the further digital signature to a specified recipient.

25 32. A digital witnessing system, comprising:
a witnessing server in data communication with a remote computing device;
wherein the server is adapted to receive electronically either a digitally signed document or a hash value derived from the digitally signed document from the device, to apply a further digital signature to the document or has value and to output the document or hash value.

30 33. A system as claimed in claim 32, wherein the witnessing server is adapted to timestamp the digitally signed document or hash value before applying the further digital signature.

35 34. A system as claimed in claim 32, wherein said witnessing server is arranged to apply a digital watermark or confidence mark to said document or the hash value before applying said further digital signature.

35. A system as claimed in claim 32, wherein the witnessing server receives the hash value, and the hash value is encrypted.
- 5 36. A system as claimed in claim 35, wherein the hash value comprises a digital signature used to sign the digitally signed document.