SYSTEM AND METHOD FOR RULES-BASED CONTROL OF CUSTODY OF ELECTRONIC SIGNATURE TRANSACTIONS

PRIORITY CLAIM

[0001] This application claims the benefit of U.S. Provisional Application No. 61/614,371, filed March 22, 2012.

FIELD OF THE INVENTION

[0002] The present disclosure relates to systems and methods for electronic signatures and, more particularly, to systems and methods for rules-based control of custody of electronic signature documents.

BRIEF DESCRIPTION OF THE DRAWINGS

[0003] Preferred and alternative examples of the present invention are described in detail below with reference to the following drawings:

[0004] FIGURE 1 illustrates an example block diagram of an example embodiment of an electronic signature service;

[0005] FIGURE 2 is a flow diagram of an example rules manager process according to an example embodiment; and

[0006] FIGURE 3 is a block diagram of an example computing system for implementing an electronic signature service according to an example embodiment.

DETAILED DESCRIPTION

[0007] Embodiments described herein provide enhanced computer- and network-based methods and systems for facilitating electronic signatures. Example embodiments provide an electronic signature service ("ESS") configured to facilitate the creation, storage, and management of documents and corresponding electronic signatures. Using the ESS, a first user (a "sender") can provide or upload a document to be signed ("a signature document"), while a second user (a "signer") can access, review, and sign the uploaded document.

[0008] Some embodiments of the ESS facilitate rules-based control of custody of electronic signature documents. In one embodiment, an electronic signature document includes

or is associated with custody transfer rules (or simply, "custody rules") that govern, control, or facilitate transfers of custody of an electronic signature document from one user or party to another. A custody transfer typically results in a transfer of rights or capabilities to operate upon (*e.g.*, modify, view, send, delete) an electronic signature document and/or its associated data (*e.g.*, history, form data, signature data). In some embodiments, when an electronic signature document changes custody, a first party associated with the document (*e.g.*, that created, edited, or sent the document) loses one or more previously held rights to the document while a second party gains those and possibly other rights. For example, upon custody transfer, a first user (*e.g.*, the initial document sender) may lose the right to edit or delete the document, while a second user (*e.g.*, a manager) may gain the rights to view, edit, and delete the document. The first user may in some embodiments or configurations retain some rights, such as "read only" access allowing the first user to view the document.

[0009] Custody transfer rules may also specify conditions under which transfers of custody are to take place. For example, a sales organization may have two distinct types of users: sales representatives and sales managers. A sales representative may create an electronic signature document (or clone or copy an existing one) that represents a sales contract with a customer. Such an electronic signature document may be associated with custody transfer rules that cause custody of the document to transfer from the sales representative to the sales manager upon the occurrence of one or more events, such as when a customer completes an electronic signature, thereby closing a sale or otherwise completing a transaction. Other conditions may be specified, such as when the sales representative initially sends the electronic signature document to the customer, when a customer indicates refusal to sign the electronic signature document, when a specified amount or period of time passes, or the like.

[0010] FIGURE 1 illustrates an example block diagram of an example embodiment of an electronic signature service. In particular, FIGURE 1 depicts an ESS 110 utilized by a sender user 10 and a signer user 11 to perform an electronic signing of a signature document 20. FIGURE 1 also depicts a transferee 12 who receives custody of the signature document 20.

[0011] In the illustrated scenario, the sender 10 operates a sender client device 160 in order to provide (*e.g.*, upload, transmit) an electronic document 20 (*e.g.*, an invoice, contract, or agreement) to the ESS 110, where it is securely stored. The electronic document includes or is associated with custody rules 21 that are configured to cause custody of the document 20 to transfer from the sender 10 to the transferee 12, possibly upon the occurrence of one or more conditions. In some embodiments or configurations, the sender 10 and transferee 12 may be in or work for the same organization. For example, the sender 10 may be a sales representative while

the transferee 12 may be a sales manager or an in-house attorney who reviews and records sales contracts. In other situations, the sender 10 and transferee 12 may work for distinct organizations or entities.

[0012] The sender 10 and/or some other user (*e.g.*, an administrator) may configure the document 20 and/or the custody rules 21. For example, an administrator may interact with a user interface configured to facilitate the specification of custody rules and associated conditions. The custody rules 21 are then stored by the ESS 110 in association with the document 20. In this example, the custody rules 21 are configured to cause custody of the document 20 to transfer to the transferee upon signature by the signer 11. At this time, the sender 10 may further modify, configure, or customize the document 20, such as by changing price and quantity terms, party names, dates, and the like.

[0013] After the sender 10 configures the document 20 to his satisfaction, the signer 11 may access the document 20. In one embodiment, the sender 10 notifies the signer 11, such as by causing the ESS 110 to send to the signer 11 a message (*e.g.*, an email) that includes a reference (*e.g.*, a URL) to the document 20 stored by the ESS 110. As another example, the sender 10 may directly include the document 20 in an email or other message transmitted to the signer 11. As a further example, the document 20 may be automatically presented to the signer 11 as part of a transaction. For example, an e-commerce system may cause the document 20 to be presented or transmitted to the signer 11 during or as part of a transaction for a good/service purchased via the e-commerce system.

[0014] Typically, the signer 11 operates a Web browser or other client module executing on the signer client device 161 to access and review the document 20 via the ESS 110. For example, if the signer 11 receives an email that includes a link to the document 20, the signer can click the link to visit the ESS 110 in order review and sign the document 20. If instead the signer 11 receives the document 20 itself directly from the sender 10, opening the document will also cause the user to visit the ESS 110 to provide the required signature information. When the document 20 and related data have been reviewed (and possibly modified) to the satisfaction of the signer 11, the signer attaches (or provides an indication or instruction to attach) his electronic signature to the document 20.

[0015] Once the signing has been completed, the ESS 110 causes custody of the document 20 to change from the sender 10 to the transferee 12. At this time, the sender 10 may lose one or more rights, such as the right to view, modify, or delete the document 20. In addition, the transferee 12 may gain one or more rights, such as the right to view, modify, or delete the document 20. The transferee 12 can access and perform various operations (*e.g.*, view, modify,

delete) via the transferee client device 162. Custody transfer rules may specify custody chains or sequences of arbitrary length (*e.g.*, more than the two parties shown in this example). For example, custody of a document may transfer from a sales representative to a sales manager and thence to an in-house attorney.

[0016] In some embodiments, the document 20 may be associated with an envelope or other data structure that functions as a container that includes the document 20 (or a reference thereto) along with meta-information, including signature information, sender information (*e.g.*, names, addresses), recipient/signer information (*e.g.*, email addresses, names), and the like. Custody rules may be configured to manage access to an envelope and its related information. For example, one custody rule may specify that once the sender 10 has transferred control to the transferee 12, the sender 10 may view but not modify envelope information including the document 20. The transferee 11, in turn, may receive additional rights, such as to delete the document 20, view information added to a form associated with the document 20, clone the document 20, or the like. In some embodiments, a user may upload a file that contains information about multiple documents for which custody is to be transferred, so as to effect a bulk transfer from one party to another.

[0017] FIGURE 2 is a flow diagram of an example rules manager process 200 according to an example embodiment. The process of FIGURE 2 may be performed by the ESS 110.

[0018] The illustrated process begins at block 202, where it associates a custody transfer rule with an electronic signature document. Associating a custody rule may include storing data structure or record that relates the custody rule with the document. The custody rule itself may be a data structure or record that includes indications of the document, users impacted by the custody rule, conditions or events that trigger custody transfers, access rights impacted by the rule, or the like.

[0019] At block 204, the process, in response to occurrence of an event, transfers custody of the document based on the custody transfer rule. Transferring custody may include removing one or more access rights from the first user, and in turn, granting those access rights to a second user. Different kinds of events may trigger the transfer operation, including the presentation (*e.g.*, viewing), receipt, signature, or other operation upon or with respect to a signature document. Some events may be time based, so that custody transfers are triggered upon a passage of time or on a specified calendar day.

[0020] At block 206, the process stores information about the transfer of custody of the electronic signature document. Storing information about custody transfer may include updating

a data structure or record to reflect a new document owner, to remove rights from one user, to grant rights to another user, or the like. After block 206, the process ends.

[0021] The process may perform additional or different operations. In some embodiments, the process may also enforce access rules governed by the custody rule. For example, when the process receives an indication that a user is attempting to perform some operation (*e.g.*, view, edit, delete) with respect to the signature document or its meta-data, the process may allow or disallow the operation based on a determination whether the user has the appropriate access rights to perform the indicated operation.

[0022] FIGURE 3 is a block diagram of an example computing system for implementing an electronic signature service according to an example embodiment. In particular, FIGURE 3 shows a computing system 100 that may be utilized to implement an ESS 110.

[0023] Note that one or more general purpose or special purpose computing systems/devices may be used to implement the ESS 110. In addition, the computing system 100 may comprise one or more distinct computing systems/devices and may span distributed locations. Furthermore, each block shown may represent one or more such blocks as appropriate to a specific embodiment or may be combined with other blocks. Also, the ESS 110 may be implemented in software, hardware, firmware, or in some combination to achieve the capabilities described herein.

[0024] In the embodiment shown, computing system 100 comprises a computer memory ("memory") 101, a display 102, one or more Central Processing Units ("CPU") 103, Input/Output devices 104 (*e.g.*, keyboard, mouse, CRT or LCD display, and the like), other computer-readable media 105, and network connections 106 connected to a network 150. The ESS 110 is shown residing in memory 101. In other embodiments, some portion of the contents, some or all of the components of the ESS 110 may be stored on and/or transmitted over the other computer-readable media 105. The components of the ESS 110 preferably execute on one or more CPUs 103 and manage electronic signature processes including custody transfers as described herein. Other code or programs 130 (*e.g.*, an administrative interface, a Web server, and the like) and potentially other data repositories, such as data repository 120, also reside in the memory 101, and preferably execute on one or more CPUs 103. Of note, one or more of the components in FIGURE 3 may not be present in any specific implementation. For example, some embodiments may not provide other computer readable media 105 or a display 102.

[0025] The ESS 110 includes a service manager 111, a user interface ("UI") manager 112, an electronic signature service application program interface ("API") 113, a rules manager 114, and an electronic signature service data store 115.

[0026] The ESS 110, via the service manager 111 and related logic, generally performs electronic signature-related functions for or on behalf of users operating a sender client device 160, a signer client device 161, and a transferee client device 162. In one embodiment, a sender operating the sender client device 160 provides (*e.g.*, transmits, uploads, sends) a document to be electronically signed to the ESS 110. The ESS 110 stores the document securely in data store 115. Secure document storage may include using cryptographic techniques to detect document tampering, such as generating hashes, message digests, or the like. In some embodiments, the document is stored as part of (or in association with) an "envelope" that is used to track and record information about the document as it progresses through its lifecycle of creation, transfer, signature, completion, and the like.

[0027] A signer operating the signer client device 161 then accesses, reviews, and signs the document stored by the ESS 110. In some embodiments, the ESS 110 transmits images or some other representation of the document to the signer client device 161, which in turn transmits signature data including an indication of the signer's signature (or intent to sign) to the ESS 110. The ESS 110 then securely stores the provided signature data in association with the document in the data store 115.

[0028] The rules manager 114 facilitates custody transfers of electronic signature documents as discussed herein. Initially, a sender or other user operating the sender client device 160 may associate custody transfer rules with an electronic signature document stored in the data store 115. The rules manager 114 tracks and executes the specified rules as appropriate. For example, if a rule indicates custody transfer upon document signature, the rules manager 114 monitors the document and, in response to a received signature, modifies (or causes to be modified) data structures or other records that specify or control access rights or operations associated with the document. In particular, access rights may be removed or disassociated from a first user. In addition or instead, the same or different access rights may be granted or otherwise associated with a second user. In some embodiments, custody transfers may occur between groups of users.

[0029] A custody transfer rule may be represented as a data structure, record in a database, or similar. The custody transfer rule may include indications of users that are impacted by the rule, events that trigger the rule, and access rights (*e.g.*, view, modify, delete) that are shifted based on the rule and one or more events.

[0030] The UI manager 112 provides a view and a controller that facilitate user interaction with the ESS 110 and its various components. For example, the UI manager 112 may provide interactive access to the ESS 110, such that users can upload or download documents for

signature, create and/or configure custody rules associated with or incorporated into signature documents, and the like. In some embodiments, access to the functionality of the UI manager 112 may be provided via a Web server, possibly executing as one of the other programs 130. In such embodiments, a user operating a Web browser (or other client) executing on one of the client devices 160-162 can interact with the ESS 110 via the UI manager 112.

[0031] The API 113 provides programmatic access to one or more functions of the ESS 110. For example, the API 113 may provide a programmatic interface to one or more functions of the ESS 110 that may be invoked by one of the other programs 130 or some other module. In this manner, the API 113 facilitates the development of third-party software, such as user interfaces, plug-ins, news feeds, adapters (*e.g.*, for integrating functions of the ESS 110 into Web applications), and the like. In addition, the API 113 may be in at least some embodiments invoked or otherwise accessed via remote entities, such as a third-party system (not shown), to access various functions of the ESS 110. For example, a customer relationship management system may push or otherwise import customer data and/or agreements into the ESS via the API 113.

[0032] The data store 115 is used by the other modules of the ESS 110 to store and/or communicate information. The components of the ESS 110 use the data store 115 to record various types of information, including documents, signatures, custody rules, and the like. Although the components of the ESS 110 are described as communicating primarily through the data store 115, other communication mechanisms are contemplated, including message passing, function calls, pipes, sockets, shared memory, and the like.

[0033] The ESS 110 interacts via the network 150 with client devices 160-162. The network 150 may be any combination of one or more media (*e.g.*, twisted pair, coaxial, fiber optic, radio frequency), hardware (*e.g.*, routers, switches, repeaters, transceivers), and one or more protocols (*e.g.*, TCP/IP, UDP, Ethernet, Wi-Fi, WiMAX) that facilitate communication between remotely situated humans and/or devices. In some embodiments, the network 150 may be or include multiple distinct communication channels or mechanisms (*e.g.*, cable-based and wireless). The client devices 160-162 include personal computers, laptop computers, smart phones, personal digital assistants, tablet computers, and the like.

[0034] In an example embodiment, components/modules of the ESS 110 are implemented using standard programming techniques. For example, the ESS 110 may be implemented as a "native" executable running on the CPU 103, along with one or more static or dynamic libraries. In other embodiments, the ESS 110 may be implemented as instructions processed by a virtual machine that executes as one of the other programs 130. In general, a

range of programming languages known in the art may be employed for implementing such example embodiments, including representative implementations of various programming language paradigms, including but not limited to, object-oriented (*e.g.*, Java, C++, C#, Visual Basic.NET, Smalltalk, and the like), functional (*e.g.*, ML, Lisp, Scheme, and the like), procedural (*e.g.*, C, Pascal, Ada, Modula, and the like), scripting (*e.g.*, Perl, Ruby, Python, JavaScript, VBScript, and the like), and declarative (*e.g.*, SQL, Prolog, and the like).

[0035] The embodiments described above may also use either well-known or proprietary synchronous or asynchronous client-server computing techniques. Also, the various components may be implemented using more monolithic programming techniques, for example, as an executable running on a single CPU computer system, or alternatively decomposed using a variety of structuring techniques known in the art, including but not limited to, multiprogramming, multithreading, client-server, or peer-to-peer, running on one or more computer systems each having one or more CPUs. Some embodiments may execute concurrently and asynchronously, and communicate using message passing techniques. Equivalent synchronous embodiments are also supported. Also, other functions could be implemented and/or performed by each component/module, and in different orders, and by different components/modules, yet still achieve the described functions.

[0036] In addition, programming interfaces to the data stored as part of the ESS 110, such as in the data store 118, can be available by standard mechanisms such as through C, C++, C#, and Java APIs; libraries for accessing files, databases, or other data repositories; through scripting languages such as XML; or through Web servers, FTP servers, or other types of servers providing access to stored data. The data store 118 may be implemented as one or more database systems, file systems, or any other technique for storing such information, or any combination of the above, including implementations using distributed computing techniques.

[0037] Different configurations and locations of programs and data are contemplated for use with techniques described herein. A variety of distributed computing techniques are appropriate for implementing the components of the illustrated embodiments in a distributed manner including but not limited to TCP/IP sockets, RPC, RMI, HTTP, Web Services (XML-RPC, JAX-RPC, SOAP, and the like). Other variations are possible. Also, other functionality could be provided by each component/module, or existing functionality could be distributed amongst the components/modules in different ways, yet still achieve the functions described herein.

[0038] Furthermore, in some embodiments, some or all of the components of the ESS 110 may be implemented or provided in other manners, such as at least partially in firmware

and/or hardware, including, but not limited to one or more application-specific integrated circuits ("ASICs"), standard integrated circuits, controllers executing appropriate instructions, and including microcontrollers and/or embedded controllers, field-programmable gate arrays ("FPGAs"), complex programmable logic devices ("CPLDs"), and the like. Some or all of the system components and/or data structures may also be stored as contents (*e.g.*, as executable or other machine-readable software instructions or structured data) on a computer-readable medium (*e.g.*, as a hard disk; a memory; a computer network or cellular wireless network or other data transmission medium; or a portable media article to be read by an appropriate drive or via an appropriate connection, such as a DVD or flash memory device) so as to enable or configure the computer-readable medium and/or one or more associated computing systems or devices to execute or otherwise use or provide the contents to perform at least some of the described techniques. Some or all of the system components and data structures may also be stored as data signals (*e.g.*, by being encoded as part of a carrier wave or included as part of an analog or digital propagated signal) on a variety of computer-readable transmission mediums, which are then transmitted, including across wireless-based and wired/cable-based mediums, and may take a variety of forms (*e.g.*, as part of a single or multiplexed analog signal, or as multiple discrete digital packets or frames). Such computer program products may also take other forms in other embodiments. Accordingly, embodiments of this disclosure may be practiced with other computer system configurations.

[0039] It should be apparent to those skilled in the art that many more modifications besides those already described are possible without departing from the inventive concepts herein. Moreover, in interpreting both the specification and the claims, all terms should be interpreted in the broadest possible manner consistent with the context. In particular, the terms "includes," "including," "comprises," and "comprising" should be interpreted as referring to elements, components, or steps in a non-exclusive manner, indicating that the referenced elements, components, or steps may be present, or utilized, or combined with other elements, components, or steps that are not expressly referenced. Where the specification claims refers to at least one of something selected from the group consisting of A, B, C .... and N, the text should be interpreted as requiring one or more elements from the set {A, B, C, ... N}, and not N in addition to one or more elements from the set {A, B, C}.

[0040] All of the above-cited references, including U.S. Provisional Application No. 61/614,371, filed March 22, 2012, entitled "SYSTEM AND METHOD FOR RULES-BASED CONTROL OF CUSTODY OF ELECTRONIC SIGNATURE TRANSACTIONS" are incorporated herein by reference in their entireties. Where a definition or use of a term in an

incorporated reference is inconsistent with or contrary to the definition or use of that term provided herein, the definition or use of that term provided herein governs.

[0041] While the preferred embodiment of the invention has been illustrated and described, as noted above, many changes can be made without departing from the spirit and scope of the invention. Accordingly, the scope of the invention is not limited by the disclosure of the preferred embodiment.

[0042] The embodiments of the invention in which an exclusive property or privilege is claimed are defined as follows:

1. A method for facilitating custody transfers of electronic signature documents, comprising:

associating a custody transfer rule with an electronic signature document stored by an electronic signature service, wherein the custody transfer rule is configured to cause custody of the electronic signature document to transfer from a first user to a second user;

in response to occurrence of an event, transferring custody of the electronic signature document from the first user to the second user, by:

removing from a first user an access right with respect to the electronic signature document; and

granting to the second user an access right with respect to the electronic signature document; and

storing in the electronic signature service information about the transfer of custody of the electronic signature document.

2. The method of claim 1, wherein the event is presentation of the electronic signature document to a third user for signature.

3. The method of claim 1, wherein the event is receipt of signature of the electronic signature document by a third user.

4. The method of claim 1, wherein removing from the first user the access right includes removing a right to modify the electronic signature document.

5. The method of claim 1, wherein removing from the first user the access right includes removing a right to delete the electronic signature document.

6. The method of claim 1, wherein granting to the second user the access right includes granting a right to modify the electronic signature document and/or a right to delete the electronic signature document.

7. The method of claim 1, further comprising monitoring the electronic signature document for the occurrence of the event.

8. The method of claim 1, wherein after transferring custody of the electronic signature document from the first user to the second user, the first user retains rights to view the electronic signature document and corresponding signature information, including signer information, date information, history information, and form data entered by the signer.

9. The method of claim 1, wherein associating the custody transfer rule includes receiving an indication of the custody transfer rule via an administrative user interface module, along with an indication of the first and second user and an indication of one or more events upon which custody of the electronic signature document will transfer from the first to the second user.

10. A computer-readable medium including contents that, when executed by a computing system, facilitate custody transfers of electronic signature documents, by performing a method comprising:

associating a custody transfer rule with an electronic signature document stored by an electronic signature service, wherein the custody transfer rule is configured to cause custody of the electronic signature document to transfer from a first user to a second user;

in response to occurrence of an event, transferring custody of the electronic signature document from the first user to the second user, by:

removing from a first user an access right with respect to the electronic signature document; and

granting to the second user an access right with respect to the electronic signature document; and

storing in the electronic signature service information about the transfer of custody of the electronic signature document.

11. The computer-readable medium of claim 10 wherein the contents are instructions that when executed cause the computing system to perform the method.

12. The computer-readable medium of claim 10, further comprising transmitting an email to a third user, the email including a link operable to access the electronic signature document at the electronic signature service.

13. The computer-readable medium of claim 12, wherein the event is the transmitting of the email to the third user.

14. The computer-readable medium of claim 12, further comprising receiving an indication that the third user has activated the link to access the electronic signature document.

15. The computer-readable medium of claim 14, wherein the event is the received indication that the third user has activated the link.

16. The computer-readable medium of claim 14, further comprising receiving an indication that the user has signed the electronic signature document, and wherein the event is the received indication that the third user has signed the electronic signature document.

17. A computing system configured to facilitate custody transfers of electronic signature documents, comprising:

a memory;

a processor; and

a module that is stored on the memory and that is configured, when executed by the processor, to:

associate a custody transfer rule with an electronic signature document stored by an electronic signature service, wherein the custody transfer rule is configured to cause custody of the electronic signature document to transfer from a first user to a second user;

in response to occurrence of an event, transfer custody of the electronic signature document from the first user to the second user, by:

remove from a first user an access right with respect to the electronic signature document; and

grant to the second user an access right with respect to the electronic signature document; and

store in the electronic signature service information about the transfer of custody of the electronic signature document.

18. The computing system of claim 17, wherein the custody transfer rule specifies a period of time, and wherein the event is passage of the specified period of time.

19. The computing system of claim 17, wherein the custody transfer rule indicates the first user and the second user and specifies, for each of multiple operations, whether each of the first and second user can perform the operation before and after the occurrence of the event, wherein

the multiple operations include viewing, modifying, and deleting information related to the electronic signature document.

20. The computing system of claim 19, wherein the custody transfer rule further indicates multiple events and, for each event, corresponding custody transfers that are to be performed.