

ONLINE SIGNATURE IDENTITY AND VERIFICATION IN COMMUNITY

PRIORITY CLAIM

[0001] This application claims the benefit of U.S. Provisional Application Serial No. 61/507,892 filed July 14, 2011, the contents of which are incorporated by reference.

FIELD OF THE INVENTION

[0002] The present disclosure relates to methods and systems for electronic signatures and, more particularly, to methods and systems for managing electronic signature identity cards.

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 that provides an electronic identity card;

[0005] FIGURES 2A-2E illustrate example electronic identity cards and related user interface aspects according to example embodiments;

[0006] FIGURE 3 is a flow diagram of an example electronic identity card management process; and

[0007] FIGURE 4 is a block diagram of an example computing system for implementing an electronic signature service according to an example embodiment.

DETAILED DESCRIPTION

[0008] Embodiments described herein provide enhanced computer- and network-based methods and systems for electronic identity/identification (“EID”) cards. Example embodiments provide an electronic signature service (“ESS”) configured to facilitate management of electronic identity cards. In some embodiments, an EID card is associated with a user (or “signer”) and includes, aggregates, links, or otherwise combines information about the user obtained from multiple sources and of multiple distinct types to form or represent a “social signature” associated with the user. Example information may include personal information about the user (*e.g.*, name, address, occupation, picture), electronic signature service usage/statistical information (*e.g.*, number and types of documents signed using the ESS, number and types of authentication challenges passed), and/or social networking information (*e.g.*, links to identities on one or more social networking or messaging services).

[0009] The described EID card adds a new depth of personalization to an electronic signature. In some embodiments, the EID card displays a signer’s information, how often the signer has signed and sent documents for signature, and authentication history. In further embodiments, geo-location features are provided. For example, the EID card may capture or otherwise represent the exact (or approximate) geo-location of where a signer signed for added security. As another example, users may be provided with the ability to view the location of the last document signed from any signer through a geo-location subsystem of the ESS. Also, “badges” may be associated with an EID card to indicate one or more qualities or characteristics about the associated signer, such as environmental/ecological commitment or achievement (*e.g.*, based on the number of

times the signer has signed a document electronically instead of on paper), travel profiles (e.g., the number of different countries from which the signer has signed documents), and the like.

[0010] The described techniques provide an EID card that is much more than a signature. More particularly, an EID card provides additional information about a signer and validates or further authenticates the identity of the signer. Using EID cards, senders (e.g., parties who provide documents for signature) and signers can see how often the signer has authenticated, how often they use the ESS, a picture of the signer, the signer's contact information, and the like.

[0011] In some embodiments, the ESS determines a "trust graph," which reflects or otherwise identifies a network of trust connecting two or more persons who are in some way related via the ESS or other related systems. For example, a trust graph may be based on relationships such as those that are formed when a first user signs a document provided by a second user. Once that occurs, a trust relationship between the first and second user can be represented and stored by the ESS. Such a relationship may be further strengthened when additional signature events take place between the first and second user. Furthermore, relationships can be specified by a user, such as by identifying other persons that are trusted by the user. Users may specify relationships manually or by importing such information from various electronic sources, including address books, chat logs, social networks, and the like. In addition, the EID card can be used as a vehicle for surfacing or otherwise presenting information about a signer's trust graph. The ESS,

via the use of EID cards, can thus provide a wide-ranging network within which trusted transactions can be performed.

[0012] FIGURE 1 illustrates an example block diagram of an example embodiment of an electronic signature service that provides an electronic identity card. In particular, FIGURE 1 depicts an electronic signature service 110 utilized by a sender user 10 and a signer user 11 to generate an electronic signature card and to associate the generated card with an electronic signature document.

[0013] The ESS 110 facilitates the creation of electronic signature documents and the association of electronic signatures therewith. For example, the sender 10 may operate a sender client device 160 to provide (e.g., transmit, upload, send) a document 20 to be electronically signed to the ESS 110, where it is securely stored. The document 20 may be or include a contract, agreement, purchase order, or the like. The signer 11 operates a signer client device 161 to access, review, and/or sign the document 20 stored by the ESS 110. In some embodiments, the ESS 110 transmits images or some other representation of the document 20 to the signer client device 161, which in turn transmits an indication of the signer's signature (or intent to sign) to the ESS 110. The ESS 110 then securely stores the signer's signature in association with the document 20.

[0014] The ESS 110 also performs electronic identity card-related functions for or on behalf of the users 10 and 11. For example, the signer 11, operating the signer client device 161, may interact with the ESS 110 to create an EID card 21 that is stored and managed by the ESS 110. To create the EID card 21, the signer 11 may provide one or

more personal information items, including name, address, occupation, telephone number, picture, or the like.

[0015] The ESS 110 may augment the EID card 21 with social networking information related to the signer 11. For example, when creating the EID card 21, the signer 11 may provide credentials (e.g., username and password) associated with a social network maintained by some third-party social networking system. Using the provided credentials, the ESS 110 may then obtain social network information 30 about the signer and his social network via an API or other facility provided by the social networking system. The obtained information 30 may be stored as part of (or in association with) the signer's EID card 21.

[0016] The ESS 110 may further augment the EID card 21 with activity information 31. The activity information 31 may include information about the activities of the signer 11 with respect to the ESS 110 and/or other systems or services. For example, the ESS 110 may track the number of documents signed by the signer 11, and store that number as part of (or in association with) the EID card 21. The ESS 110 may also include (or otherwise access) a geo-location facility, used to track the location of the signer 11 as he engages in activities with the ESS 110. The geo-location facility may access or otherwise obtain information from the client device 161, such as fine-grained position information provided by a GPS receiver. Coarser-grained information may also or instead be used, such as may be provided by a communication system used by the client device 161 (e.g., carrier system for a mobile phone or other device).

[0017] In addition, the ESS 110 may track authentication activities engaged in by the signer 11, such as the number and type of authentication challenges met by the signer 11, in order to generate a score or other measure (e.g., history) reflecting a level or degree of the signer's authentication and/or experience. Information about such activities may then be presented or provided as part of the signer's EID card 21.

[0018] Upon creating the EID card 21, a reference to the created EID card 21 may be included as part of a document signed by a signer 11. For example, when the ESS 110 provides (e.g., transmits) a representation of a signed document to the sender 10, it may include information that directly or indirectly (e.g., via a URL) represents the signer's EID card 21. For example, the signed document may include an image that resembles a physical identity card and that includes at least some of the information of the EID card 21. The image or other representation may be active (e.g., clickable), such that additional information may be provided when selected or activated by the sender 10 or other user. In some embodiments, the EID card 21 is assigned or associated with a unique uniform resource locator (URL). The URL may be used by the card holder and/or other users to access, view, and/or modify the details of the EID card 21.

[0019] The EID card 21 may be made available in other contexts besides electronic signature documents. For example, the signer 11 may include a URL or other link to the EID card 21 on his social networking profile page, as part of his email signature, or the like.

[0020] FIGURES 2A-2E illustrate example electronic identity cards and related user interface aspects according to example embodiments.

[0021] FIGURE 2A illustrates an example electronic identity card 200 for a user. The card 200 is a graphical representation of a user's electronic identity card information. The card 200 may be displayed in various contexts, such as in association with a signed electronic document being viewed by the sender 10, as described with respect to FIGURE 1, above. The card 200 includes personal information about the signer/card holder, including the card holder's name, age, address, email, phone number, image, identification number, and voice print. Access to some or all of the signer information may be restricted. In this example, the card holder's address is shown in association with a padlock icon, indicating that the card holder does not want others to be able to view this information. In some embodiments, a viewer having appropriate credentials (*e.g.*, a password) may access restricted information such as the card holder's address in this example. The voice print is an audio recording created by the card holder when the card was created. A user may access the voice print to hear the voice of the card holder, which may provide additional assurance that the card is legitimate or otherwise actually associated with the indicated person.

[0022] The illustrated card 200 also includes signature information. The signature information includes signature authority level, signature date (*e.g.*, the date the signature was applied by the card holder to the associated signature document), signature pages signed (*e.g.*, a total number of pages signed by the card holder), an authentication level, and a signature image (the text "Regina P. Brown" represented in cursive). Clicking on the signature image will cause the ESS to validate the signature and/or card 200, such as by indicating that the card holder does not have (or no longer has) a valid or active

account with the service. The authentication level indicates what level and/or type of authentication has been used to verify the identity of the card holder. Authentication levels are discussed in more detail with respect to FIGURE 2D, below.

[0023] The illustrated signature authority level represents the card holder's authority level with respect to a particular organization. In some embodiments, an administrative user of a company or other organization may select users from a list and set their signature authority. For some users, this signature authority may be none or zero, meaning that they may not sign for any company-related purposes. If so, a reference to an alternative person who does have signatory authority with respect to matters handled by the user may be included. In such cases, when asked to sign a document, the card holder may reassign the document to the alternative person (and no other person) for signature. For some users it may be defined as or based on a monetary value (*e.g.*, up to \$10,000) or as a text string describing the type of contract or document. For other users, the signature authority may be total or complete. The signature authority levels may be enforced by the ESS, such as by refusing to allow users with limited signatory authority (*e.g.*, under \$1,000) to sign certain documents (*e.g.*, a purchase order in excess of \$1,000).

[0024] The card 200 further includes social networking information. The card holder has the option of associating one or more social networking services with her card. In this example, the card 200 includes icons (or other user selectable controls, such as buttons) of various associated social networking websites at the bottom of the card 200. The illustrated icons can be used to further validate the card holder's identity. A user who is viewing the card 200 may click on any of these icons to access the card holder's profile

on the corresponding social networking website. The card holder may also integrate the card with her social networks, such as by including a link to the card on her profile page of a social network.

[0025] FIGURE 2B illustrates an example electronic identity card 210 for a document. The card 210 is a graphical representation of a document's identity and signature information. The card 210 may be displayed in various contexts, such as via a link embedded within or associated with a signed electronic document. The card 210 may be used to validate the associated document's authenticity.

[0026] The card 210 includes document specifications, including document name, document identifier, number of pages, date sent, and date signed. The card 210 further includes signer information, including signer name, signer email address, authentication level, and signature image. The electronic identity card for the signer may be accessed via a link or other control. For example, upon clicking the signature image, the electronic identity card 200 described with respect to FIGURE 2A may be displayed.

[0027] The card 210 further includes a validation section. The validation section includes controls that may be used to validate the associated document. For example, using the illustrated controls, a user can upload the original document and check if the document matches. The hash of both the documents will be compared by the ESS, which will then return an indication of whether or not the document is valid. The user may then also have the option to delete the document and/or upload it again (e.g., at a later date) to validate.

[0028] The card 210 further includes a download section. Using controls in the download section, a user can download a copy of the document (with or without a certificate of completion) from the ESS.

[0029] FIGURE 2C illustrates an electronic identity card management screen 220. The screen 200 includes controls that can be used by an account holder or other user to manage their electronic identity card, such as that described with respect to FIGURE 2A, above. The screen 200 includes and displays card information, including personal information (*e.g.*, name, address, signature, email, image) and activity information (*e.g.*, document signature history, document/envelope sender history).

[0030] The user may interact with the screen 220 in order to edit or modify the card information and/or properties. In this example, the user has clicked on the “Edit Display Settings” link, which causes the display settings control 225 to be displayed. The control 225 enables the user to select what portions or elements of his electronic identity card to display, such as the entire card, company/title information, address/phone information, and/or usage history information. In this manner, the user can restrict access to some or all information that is part of his electronic identity card.

[0031] FIGURE 2D illustrates an example electronic identity card 230 according to another embodiment. The card 230 is similar to the card 200 describe above. However, the card 230 also displays an authentication history 231. The history 231 displays one or more authentication events and associated dates and mechanisms (*e.g.*, email, phone, password). The authentication history 231 may be expanded to display a

history browser/viewer 235 that provides a more comprehensive view of the user's authentication history.

[0032] The illustrated card 230 also includes badges 232. In some embodiments, badges may be associated with users (and displayed on their identity cards), in order to indicate properties of the user. In this example, one of the badges 232 (labeled “green profile badge”) iconically indicates a level of environmental/ecological commitment or impact associated with the user, based on the number of documents electronically processed or signed via the ESS, thereby reducing the amount of paper, printer, and energy resources used in association with paper-based signatures. Badges may have different shades and/or colors to indicate a level. For example, a darker shade of green used in a green profile badge may indicate a larger number of electronic signature events than a lighter shade.

[0033] The badges 232 also include an authentication level badge. The authentication level badge iconically indicates an authentication level associated with the user. Some embodiments have a hierarchy of authentication levels, based on the number and/or type of authentication mechanisms used to verify user identity, including based on one or more of email, short message service (SMS), access code, age, third-party verification, phone, and the like. The corresponding badge may have different colors, such as gold to indicate the highest level, silver to indicate the next highest level, and bronze to indicate the lowest level.

[0034] FIGURE 2E illustrates authentication mechanisms provided by one embodiment. In particular, FIGURE 2E illustrates three distinct selection scenarios 240,

243, and 246 in which one or more authentication mechanisms are selected for association with a document and/or electronic identity card provided by an example embodiment. For example, a sender may select and associate one or more authentication mechanisms with a document that is to be signed by one or more signers. Similarly, one or more of the illustrated authentication mechanisms may be used by a signer to verify their identity when signing a document and/or creating an electronic identity card.

[0035] In scenario 240, a user has selected email identification and phone authentication. In some embodiments, email authentication is the default identification/authentication method. Email authentication provides a baseline level of authentication, in that the user operating the identified email account is quite likely the intended recipient or signer of a document.

[0036] The phone authentication option asks the user to select or type a phone number to use for authentication. The recipient is provided with a validation code (e.g., in email or other more secure communication). Later, during a signature transaction, the ESS places a call to the number. After answering the phone, the recipient is prompted to enter the validation code and speak their name. The illustrated phone numbers may be automatically obtained from an address book associated with the sender and/or the recipient. Phone authentication may be considered to be a more rigorous authentication method than email authentication.

[0037] Also shown, but not selected in this scenario, is access code authentication. In this mechanism, the user types an access code (e.g., upper case or lower case letters, numbers, and special characters) that is also provided to the intended

recipient. Later, when the recipient reviews and/or signs a document, he must provide the access code (e.g., via a Web form entry) in order to complete the transaction.

[0038] In scenario 243, a user has selected identity check authentication. The identity check option asks the recipient to provide some initial personal information (current address is required, but there may be other optional information the recipient can enter) and then answer a set of questions before the recipient can access a signature document. The questions are based on data available in public records, such as past or present residence addresses of the recipient. In some embodiments, the identity check mechanism may be provided by a third party, such as RSA.

[0039] In scenario 246, a user has selected social identity check authentication. The social identity check option asks the recipient to login to a specified (or any) social identity service provider including Facebook, Yahoo, Google, Twitter, OpenID, LiveID, LinkedIn, Salesforce or the like. Once the recipient successfully logs into the specified social identity provider, the recipient will be permitted to view/sign the signature document.

[0040] Some embodiments provide a scoring mechanism that may be used to indicate a level of trust or experience associated with a card holder. The score may be based on one more of the following: whether the user is validated/authenticated or not, the level or type of validation/authentication used, the date of the last signature, the date of the last login, the number of pages signed, and the like. The score may be graphically represented on an electronic identity card, by way of color, icons, numerals, letter grades, badges, or the like.

[0041] In one embodiment, the score is based on points that are awarded for actions undertaken by a user during signing, sending, authentication, signing authority, connections to other trusted networks, and the like.

[0042] Points based on document sending may include points for the first envelope sent by the user, points for subsequent documents (*e.g.*, the next 100), and/or points for reaching milestones (*e.g.*, every 100th document). The number of points may vary based on the total number of sending events (*e.g.*, one point per document for documents 1-100, 0.1 point per document for documents 100-500). Points may also be based on the number of total pages sent by the user (*e.g.*, 0.01 points per page). Points may also be based on the number of unique or distinct recipients (*e.g.*, 1 points for each distinct recipient, 5 points for each recipient that has not previously received a document). Points may also be based on frequency or recency of use (*e.g.*, deduct one point for every 30 days that a document is not sent). Other factors may include the number and type of authentication methods used (*e.g.*, one point for sending a document that uses an authentication method other than email address); use of a system API; and/or use of a particular system feature (*e.g.*, bulk sending, mobile device interface).

[0043] Points based on document signature may include or be based on: signature adoption; hand drawing a signature rather than using a preselected signature; selecting a different system signature than the default signature; acceptance of the terms and conditions; the number of documents signed; signing milestones (*e.g.*, for the 500th document); number of pages signed; frequency or recency of signature (*e.g.*, subtract one

point if no signature in the last 90 days); and/or special features used (*e.g.*, document reassignment, carbon copy request, acknowledgement receipt).

[0044] Points based on authentication actions or events may include or be based on: initial authentication (*e.g.*, for the first authentication event); use of email authentication; total number of authentications; authentication failures; use of access code authentication; use of identity check authentication; use of phone authentication; use of age verification; use of social network identification; or the like. As different authentication mechanisms are regarded as more secure or rigorous, use of different mechanisms may be rewarded differently to reflect this hierarchy or ordering. For example, phone authentication may be awarded five points, whereas email authentication may be awarded one point, thereby reflecting the actual or perceived security levels associated with each of those mechanisms.

[0045] FIGURE 3 is a flow diagram of an example electronic identity card management process. The illustrated process may be performed by one or more modules of the ESS 110 described herein. Other embodiments may perform fewer or additional operations than those illustrated here.

[0046] The process begins at block 302, where it receives personal information about a user. Personal information may include one or more of name, address, telephone number, email address, photo, or the like.

[0047] At block 304, the process receives activity information about actions of the user. Activity information may include actions performed with respect to the

electronic signature service, such as signature events, document sending, authentication events, or the like.

[0048] At block 306, the process generates an electronic identity card based on the personal information and the activity information. Generating the electronic identity card may include creating or updating a card based on the information received. In some cases, such as with the user's address, it may be included in the card directly. In other cases, the process may aggregate or analyze the received information. For example, the process may determine a score or other aggregate information based on the user's activities (e.g., types or number of authentication challenges met). The determined score may then be included in the card to indicate a level of trust, history, or experience with the electronic signature service.

[0049] At block 308, the process provides information about the generated electronic identity card. Providing information about the generated card may include providing (e.g., transmitting, sending) a textual or graphical representation of the card, or a reference thereto. In some cases, the card may be associated along with an electronic signature document, such as by including a URL or other reference to the card in the document.

[0050] FIGURE 4 is a block diagram of an example computing system for implementing an electronic signature service according to an example embodiment. In particular, FIGURE 4 shows a computing system 100 that may be utilized to implement an electronic signature service 110.

[0051] Note that one or more general purpose or special purpose computing systems/devices may be used to implement the electronic signature service 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 electronic signature service 110 may be implemented in software, hardware, firmware, or in some combination to achieve the capabilities described herein.

[0052] 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 electronic signature service 110 is shown residing in memory 101. In other embodiments, some portion of the contents, some or all of the components of the electronic signature service 110 may be stored on and/or transmitted over the other computer-readable media 105. The components of the electronic signature service 110 preferably execute on one or more CPUs 103 and manage electronic signature processes and EID cards 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 4 may not be present in

any specific implementation. For example, some embodiments may not provide other computer readable media 105 or a display 102.

[0053] The electronic signature service 110 includes an electronic identity (“EID”) card manager 111, a user interface (“UI”) manager 112, an electronic signature service application program interface (“API”) 113, and an electronic signature service data store 115.

[0054] The EID manager 111 includes logic configured to perform identity card management functions of the ESS 110, as described above. Functions of the EID manager 111 may include generating new identity cards, managing or modifying existing identity cards, authenticating users (or providing access to related authentication services), identity card use/activity tracking, scoring, and the like.

[0055] The UI manager 112 provides a view and a controller that facilitate user interaction with the electronic signature service 110 and its various components. For example, the UI manager 112 may provide interactive access to the electronic signature service 110, such that users can upload or download documents for signature, create and manage EID cards, 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 or 161 can interact with the electronic signature service 110 via the UI manager 112.

[0056] The API 113 provides programmatic access to one or more functions of the electronic signature service 110. For example, the API 113 may provide a

programmatic interface to one or more functions of the electronic signature service 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 electronic signature service 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 the third-party system 165, to access various functions of the electronic signature service 110. For example, a social networking service executing on the system 165 may obtain information about EID cards managed by the ESS 110 via the API 113.

[0057] The data store 115 is used by the other modules of the electronic signature service 110 to store and/or communicate information. The components of the ESS 110 use the data store 115 to securely store or record various types of information, including documents, signatures, EID cards, activity information, 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.

[0058] The electronic signature service 110 interacts via the network 150 with client devices 160 and 161, and third-party systems 165. The third-party systems 165 may include social networking systems, third-party authentication or identity services, identity information providers (e.g., credit bureaus), or the like. 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 and 161 include personal computers, laptop computers, smart phones, personal digital assistants, tablet computers, and the like.

[0059] In an example embodiment, components/modules of the electronic signature service 110 are implemented using standard programming techniques. For example, the electronic signature service 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 electronic signature service 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).

[0060] 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.

[0061] In addition, programming interfaces to the data stored as part of the electronic signature service 110, such as in the data store 115, 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.

[0062] Different configurations and locations of programs and data are contemplated for use with techniques of 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.

[0063] Furthermore, in some embodiments, some or all of the components of the electronic signature service 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.

[0064] 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. The inventive subject matter, therefore, is not to be restricted except in the spirit of the appended claims. 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 only one element from the group, not A plus N, or B plus N, etc.

[0065] 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. Instead, the invention should be determined entirely by reference to the claims that follow.

CLAIMS

1. A method for managing electronic identity cards, comprising:
receiving personal information about a user of an electronic signature service;
receiving activity information about actions of the user on the electronic signature service;
generating an electronic identity card that includes the received personal information and the received activity information; and
providing information about the generated electronic identity card in association with a document signed by the user via the electronic signature service.
2. The method of claim 1, further comprising:
receiving social networking information about the user; and
incorporating the received social networking information into the generated electronic identity card.
3. The method of claim 2, wherein receiving the social networking information includes receiving credentials used by the user to access a social networking service.
4. The method of claim 1, wherein receiving the personal information includes receiving an indication of at least one of: a name, an address, an occupation, a telephone number, and an image of the user.
5. The method of claim 1, wherein providing the information about the generated electronic identity card includes incorporating information from the electronic identity card into a representation of the signed document, and transmitting the signed document.
6. The method of claim 1, wherein providing the information about the generated electronic identity card includes incorporating a reference to the electronic identity card into a representation of the signed document.

7. The method of claim 6 wherein the reference is a uniform resource locator that identifies a computing system configured to provide information about the electronic identity card.

8. The method of claim 1, further comprising:

tracking the activity information in response to document signature events occurring on the electronic signature service; and
incorporating statistics about the tracked activity information into the generated electronic identity card.

9. The method of claim 8 wherein tracking the activity information includes tracking at least one of: a number of documents signed by the user, a number of documents reviewed by the user, a number of documents uploaded for signature by the user, and a number of authentication challenges passed by the user.

10. The method of claim 8, further comprising:

tracking authentication challenges presented to and passed by the user;
incorporation information about the tracked authentication challenges into the generated electronic identity card; and
presenting the information about the tracked authentication challenges as part of a display of the generated electronic identity card.

11. The method of claim 10, wherein presenting the information about the tracked authentication challenges includes presenting a trust score that indicates a level of trust determined based on the information about the tracked authentication challenges.

12. A computer-readable storage medium having contents that, when executed by a computing system, facilitate management of electronic identity cards, by performing the method comprising:

receiving personal information about a user of an electronic signature service;

receiving activity information about actions of the user on the electronic signature service;
generating an electronic identity card that includes the received personal information and the received activity information; and
providing information about the generated electronic identity card in association with a document signed by the user via the electronic signature service.

13. The computer-readable storage medium of claim 12, wherein the computer-readable storage medium is a memory in the computing system, and wherein the contents are instructions in the memory that, when executed, cause the electronic signature service to perform the method.

14. The computer-readable storage medium of claim 12, wherein providing information about the generated electronic identity card includes displaying a green profile badge that indicates a level of ecological commitment based on how many times the user has used the electronic signature service to sign documents.

15. The computer-readable storage medium of claim 12, wherein providing information about the generated electronic identity card includes displaying an authentication level based on how many distinct authentication mechanisms have been used by the user to verify the user's identity, and further based on the types of the distinct authentication mechanisms.

16. A computing system configured to facilitate management of electronic identity cards, comprising:

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

receiving personal information about a user of an electronic signature service;
receiving activity information about actions of the user on the electronic signature service;
receiving social networking information about the user;
generating an electronic identity card that includes the received personal information, the received activity information, and the received social networking information; and
providing information about the generated electronic identity card in association with a document signed by the user via the electronic signature service.

17. The computing system of claim 16 wherein the module includes software instructions for execution in the memory of the computing system.

18. The computing system of claim 16 wherein the module is an electronic signature service module.

19. The computing system of claim 16 wherein the activity information location information about the user, the location information including indications of locations at which the user reviewed and/or signed an electronic signature document.

20. The computing system of claim 19, wherein the method further comprises:
receiving the indications of locations from a mobile device operated by the user to interact with the electronic signature service.