

METHOD FOR ASSOCIATING THIRD PARTY CONTENT WITH ONLINE DOCUMENT SIGNING

INVENTORS

Thomas H. Gonser
Donald G. Peterson

PRIORITY CLAIM

[0001] This application claims the benefit of U.S. Provisional Application Serial No. 61/507,910 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 associating third-party content with online electronic document signing.

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] FIGURES 2A and 2B illustrate user interface aspects according to an example embodiment;

[0006] FIGURE 3 is a flow diagram of an example dynamic form 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 dynamic signature documents. 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.

[0009] Some embodiments of the ESS support dynamic signature documents. In one embodiment, a dynamic signature document includes or is associated with at least one dynamic form field that is mapped to an associated data store. When a dynamic signature document is accessed by a signer, its dynamic form fields are automatically populated with data obtained from the associated data store. Similarly, if the signer makes any changes to a dynamic form field, the changed data may be automatically propagated (e.g., written back, transmitted, recorded, stored) back to the associated data store. For example, suppose a document includes a dynamic form field representing a current telephone number of a signer. This field may be mapped to an associated data store, such as a database that includes customer data. Then, when a signer accesses the document, the field will be automatically populated with a current telephone number of the signer obtained from the database. And if the signer, in the course of reviewing and signing the document, changes or updates his current telephone number, the changed telephone number will be propagated back to the database.

[0010] FIGURE 1 illustrates an example block diagram of an example embodiment of an electronic signature service. In particular, FIGURE 1 depicts an electronic signature service 110 utilized by a sender user 10 and a signer user 20 to perform an electronic signing of a dynamic signature document.

[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., a contract, sales order, or agreement) to the ESS 110, where it is securely stored. The electronic document includes a field 21 that is configured to include data for the document 20, such as contact information, item descriptions, quantity, date, party name, or the like. The sender 10 may configure the field 21 by associating or mapping the field to a data store, such as customer data 30 hosted by a third-party system 165. In one embodiment, the third-party system 165 is a customer relationship management (“CRM”) system that is used to store and manage information used in the sales context, including customer contact information, sales history, account information, and the like.

[0012] After configuring the form field, the sender notifies the signer 11. In some embodiments, the sender 10 causes 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 and maintained by the ESS 110. Upon receiving the message, 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. When the signer 11 accesses the document 20, the ESS 110 automatically obtains form data (e.g., a current telephone number for the

signer 11) from customer data 30 in the third-party system 165, and inserts the obtained form data into the field 21.

[0013] During review, the signer 11 may update form data, such as by changing a telephone number or other item stored in the field 21. When the document has been 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. Once the signing has been completed, the ESS 110 writes back any form data changed by the signer 11 during the course of the signing. For example, if the signer 11 updated his current telephone number in field 21, the ESS 110 will write back the changed data to the third-party system 165, where it is stored in customer data 30.

[0014] FIGURES 2A and 2B illustrate user interface aspects according to an example embodiment. FIGURE 2A illustrates a dynamic form field management screen 200. The screen 200 includes controls that are configured to create, edit, modify, or otherwise manage a dynamic form field. The screen 200 may be part of a user interface provided by an example embodiment of the ESS 110. For example, the ESS 110 may provide an administrative user interface configured to facilitate the creation and management of dynamic form fields. In one embodiment, the screen 200 may be displayed (e.g., as a Web page) via a Web browser or other client application on the sender client device 160 so that the sender 10 can create the form field 21 for inclusion with the document 20, as described with respect to FIGURE 1.

[0015] The illustrated screen 200 includes a dynamic field selection control 201, data store access parameter controls 202, and a write back control 203. By selecting

(e.g., checking) the dynamic field selection control 201, a user may indicate that the present field is a dynamic form field that is associated with a data store. The user may then further provide access parameters via the parameter controls 202. For example, the user may provide the name of a corresponding data field or object (e.g., “Opportunity”) in the data store, an account reference, and an account name. Other parameters may include access credentials (e.g., username and password), data type specification (e.g., number, text, telephone number), and the like.

[0016] In addition, the user may initiate write back functionality with respect to the present dynamic form field via the write back control 203. By selecting the control 203, the dynamic form field will write back (or cause to be written back) any changes to the form field made during a signature process.

[0017] Other properties or features of the dynamic form field may also be specified via the screen 200. For example, the user may provide, indicate, or specify a label, a tool tip (e.g., text to display upon a mouse over), an initial or default value, font details, field width and height, a regular expression pattern to which the form data must match, and a validation error message to display if entered form data does not match the regular expression pattern. In other embodiments, dynamic form fields may have additional, other, or fewer properties or features than those illustrated here.

[0018] In one embodiment, the dynamic form field of screen 200 may be automatically created by the ESS 110. For example, the ESS 110 may access a database schema or other metadata that describes the contents of the data store 30. Based on data objects or records defined by the schema, the ESS 110 may automatically generate one or

more dynamic form fields. For example, if the schema defines a customer address record (e.g., including a street address, a city, a state, and a postal code), the ESS 110 may generate a customer address dynamic form field that may be further manually modified via the screen 200 and/or included in signature documents managed by the ESS 110.

[0019] FIGURE 2B illustrates a document signature screen 210. The screen 210 may be part of a user interface provided by an example embodiment of the ESS 110. For example, the ESS 110 may provide a signer user interface configured to facilitate the review and signature of signature documents that may include dynamic form fields. In one embodiment, the screen 210 may be displayed (e.g., as a rendered Web page) via a Web browser or other client application on the signer client device 161 so that the signer 11 can review and sign the document 20, as described with respect to FIGURE 1.

[0020] The screen 210 displays a representation of a signature document 211 as well as associated controls for reviewing, modifying, and signing the document. The representation of the signature document 211 may be or include one or more images of the document 20. In this example, the document 20 is a sales order, and its representation 211 displays details of the order, including addresses, order items, and a signature block.

[0021] The screen 210 includes at least one dynamic form field control 212 and a signature control 213. When the screen 210 is prepared by the ESS 110, the dynamic form field control 212 is populated with data. In this example, the control 212 is based on field 21 and associated with a customer address that is obtained from the customer data 30. The signer 11 may review and possibly modify the customer address as well as other form elements (e.g., shipping address).

[0022] Once the signer 11 is satisfied with his review, the signer may activate the signature control 213 to provide his electronic signature or otherwise manifest his assent to the terms of the agreement represented by the displayed document. As discussed above, once the document is signed, the contents of the control 212 (if modified) may be written back to the customer data store 30. Note that the contents of the control 212 may be written back upon the occurrence of other events, such as when the signer 11 saves the document for later signature, when the signer 11 forwards the document to other parties, upon the passage of a time interval (e.g., auto save), or the like.

[0023] FIGURE 3 is a flow diagram of an example dynamic form 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.

[0024] The process begins at block 302, where it receives an indication of a dynamic form field mapped to an associated data store. Receiving the indication of the dynamic form field may include receiving a selection of the form field via an user interface configured to prepare electronic documents for signature. For example, a user may select (e.g., drag and drop) a dynamic form field from a menu of form fields for inclusion with an electronic signature document.

[0025] At block 304, the process associates the dynamic form field with an electronic signature document. Associating the dynamic form field may include embedding or incorporating the form field (or a copy thereof) into the signature document. In other embodiments, associating the dynamic form field may include adding

to the signature document a link or reference to the form field. The form field itself may be represented as some combination of instructions and/or data that is configured to perform or cause to be performed the functions associated with the form field, such as fetching and/or writing back form data, displaying its contents, responding to user input events, and the like.

[0026] At block 306, the process populates the dynamic form field with data from the data store. Populating the form field with data may include interacting with the data store to obtain the appropriate data, as specified by the dynamic form field. For example, the form field may specify a query to execute against a database, the query configured to return a particular data item (e.g., customer address). Having obtained the data item from the data store, the process stores the data item in association with the form field. In some embodiments, the process populates the dynamic form field “on demand,” that is, in response to a request to access, view, and/or sign the electronic signature document. In this manner, the form field will contain the most recent and up-to-date information from the data store. In other embodiments, the process may instead or also pre-fetch data for the dynamic form field, so that the form field will contain some information from the data store, even if the data store is inaccessible at a later time, such as when a user initiates a signature process.

[0027] At block 308, the process presents the electronic signature document to a user for signature. Presenting the electronic signature document may include transmitting the signature document or some representation thereof (e.g., page images) to a client device, where it will be rendered or displayed to a signer. When the signature document is

displayed on the client device, the dynamic form field and associated data will also be displayed.

[0028] The process may perform additional operations in other embodiments. For example, the process may write back data from the dynamic form field which has been modified by the user. As another example, the process may automatically generate one or more dynamic form fields based on a database scheme associated with the data store.

[0029] 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.

[0030] 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.

[0031] 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 dynamic signature documents 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.

[0032] The electronic signature service 110 includes a dynamic form field (“DFF”) 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.

[0033] The ESS 110 generally performs electronic signature-related functions for or on behalf of users operating a sender client device 160 and/or a signer client device 161. 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 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. 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 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 in the data store 115.

[0034] The DFF manager 111 performs dynamic form field-related functions. For example, the signer operating signer client device 161 may interact (directly or indirectly) with the DFF manager 111 to configure a dynamic form field by specifying that data for the form field be obtained from a local or remote data store, such as data repository 120 or a data store hosted by or accessed via the third-party system 165. In addition, when a dynamic signature document is accessed by a signer (or in response to other events), the DFF manager 111 may populate its dynamic form fields using data obtained from the specified data store. Furthermore, the DFF manager 111 may, upon signature (or in response to other events) write back or propagate data from dynamic form fields that have been updated by the signer.

[0035] 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/or configure dynamic form fields 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 or 161 can interact with the electronic signature service 110 via the UI manager 112.

[0036] In one embodiment, the UI manager 112 or related components are adapted to automatically configure a user interface to facilitate the generation of dynamic signature documents. For example, the UI manager 112 may interrogate or otherwise interact with a data store (e.g., a customer relationship management data store hosted by the system 165) to determine or identify a schema or other structure that describes data objects or other contents of the data store. Then, based on the identified schema, the UI manager may automatically construct or generate a collection (e.g., a palette) of dynamic form fields that are mapped to associated data objects in the data store. This collection can then be presented to a user, who can then manipulate (e.g., drag and drop) the dynamic form fields in order to associate them with signature documents, thereby creating dynamic signature documents.

[0037] 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 customer relationship management service executing on the system 165 may provide, configure, or otherwise interact with dynamic signature documents managed by the ESS 110 via the API 113.

[0038] 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 record various types of information, including documents, signatures, dynamic form fields and related data, 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.

[0039] The electronic signature service 110 interacts via the network 150 with client devices 160 and 161, and third-party systems 165. 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.

[0040] 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).

[0041] 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.

[0042] In addition, programming interfaces to the data stored as part of the electronic signature service 110, such as in the data store 115 and/or 120, 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 illustrated data stores 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.

[0043] 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.

[0044] 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.

[0045] 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.

[0046] 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 providing electronic signature documents, comprising:
 - receiving an electronic signature document and configuration data for the electronic signature document from a first user via a user interface of an electronic signature service (ESS), the configuration data including one or more dynamic form [[field]]fields comprising unpopulated fields of the electronic signature document, the one or more dynamic form fields mapped to an associated data store, the associated data store external to the ESS and comprising dynamically updated user information; and
 - in response to a request to access the electronic signature document from a second user:
 - obtaining current user data associated with the second user from the associated data store;
 - automatically populating the one or more dynamic form fields with the current user data associated with the second user obtained from the associated data store; and
 - presenting the electronic signature document including the one or more dynamic form fields populated with the current user data associated with the second user to [[a]]the second user for signature.
2. The method of claim 1, further comprising:
 - receiving an indication that data in the one or more dynamic form fields has been modified by the second user; and
 - writing back the modified data to be stored in the associated data store.
3. The method of claim 2, wherein the modified data is written back to the associated data store upon a signature operation performed by the second user.
4. The method of claim 1, wherein the configuration data for the electronic signature document received from the first user comprises a specification of data types for the one or more dynamic form fields mapped to the associated data store that provides [[a]] data values for the one or more dynamic form fields.

5. The method of claim 1, wherein the data store is hosted by a third-party customer relationship management system, and wherein the current user data associated with the second user comprises user identification data.

6. The method of claim 1, wherein presenting the electronic signature document to the second user includes transmitting an image of a portion of the electronic signature document along with a module that represents the one or more dynamic form fields and that is configured to receive input data from the second user and to transmit the received input data to the electronic signature service.

7. The method of claim 1, further comprising:

identifying a schema associated with the data store associating one or more additional dynamic form fields with the one or more dynamic form fields of the electronic signature document configuration data received from the first user;

automatically populating the one or more additional dynamic form fields with the current user data associated with the second user obtained from the associated data store; and

presenting the electronic signature document including the one or more additional dynamic form fields populated with the current user data associated with the second user to the second user for signature.

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

receiving an electronic signature document and configuration data for the electronic signature document from a first user via a user interface of an electronic signature service (ESS), the configuration data including one or more dynamic form [[field]]fields comprising unpopulated fields of the electronic signature document, the one or more dynamic form fields mapped to an associated data store, the associated data store external to the ESS and comprising dynamically updated user information; and

in response to a request to access the electronic signature document from a second user:

obtaining current user data associated with the second user from the associated data store;

automatically populating the one or more dynamic form fields with the current user data associated with the second user obtained from the associated data store; and

presenting the electronic signature document including the one or more dynamic form fields populated with the current user data associated with the second user to [[a]]the second user for signature.

9. A computing system configured to facilitate management of dynamic signature documents, comprising:

a processor;

a memory; and

a module executable via the processor using instructions stored on the memory and that, when executed by the processor, cause the computing system to:

receive an electronic signature document and configuration data for the electronic signature document from a first user via a user interface of an electronic signature service (ESS), the configuration data including one or more dynamic form [[field]]fields comprising unpopulated fields of the electronic signature document, the one or more dynamic form fields mapped to an associated data store, the associated data store external to the ESS and comprising dynamically updated user information; and

in response to a request to access the electronic signature document from a second user:

obtain current user data associated with the second user from the associated data store;

automatically populate the one or more dynamic form fields with the current user data associated with the second user obtained from the associated data store; and

present the electronic signature document including the one or more dynamic form fields populated with the current user data associated with the second user to [[a]]the second user for signature.

10. The computing system of claim 9, wherein the data store is hosted by a third-party customer relationship management system that is distinct and remote from the computing system, and wherein the current user data associated with the second user comprises identification data.
11. The computing system of claim 9, wherein the module is further configured to:
receive access credentials associated with the data store; and
obtain the current user data associated with the second user from the data store using the received access credentials.
12. The computing system of claim 9, wherein presenting the electronic signature document to the second user includes transmitting an image of a portion of the electronic signature document along with a module that represents the one or more dynamic form fields and that is configured to receive input data from the second user and to transmit the received input data to the ESS.
13. The computing system of claim 9, wherein the module is further configured to:
identify a schema associated with the data store associating one or more additional dynamic form fields with the one or more dynamic form fields of the electronic signature document configuration data received from the first user;
automatically populate the one or more additional dynamic form fields with the current user data associated with the second user obtained from the associated data store; and
present the electronic signature document including the one or more additional dynamic form fields populated with the current user data associated with the second user to the second user for signature.
14. The non-transitory computer-readable storage medium of claim 8, wherein the method further comprises:
receiving an indication that data in the one or more dynamic form fields has been modified by the second user; and
writing back the modified data to be stored in the associated data store.

15. The non-transitory computer-readable storage medium of claim 14, wherein the modified data is written back to the associated data store upon a signature operation performed by the second user.

16. The non-transitory computer-readable storage medium of claim 8, wherein the configuration data for the electronic signature document received from the first user comprises a specification of data types for the one or more dynamic form fields mapped to the associated data store that provides data values for the one or more dynamic form fields.

17. The non-transitory computer-readable storage medium of claim 8, wherein the data store is hosted by a third-party customer relationship management (CRM) system, and wherein the current user data associated with the second user comprises user identification data.

18. The non-transitory computer-readable storage medium of claim 8, wherein presenting the electronic signature document to the second user includes transmitting an image of a portion of the electronic signature document along with a module that represents the one or more dynamic form fields and that is configured to receive input data from the second user and to transmit the received input data to the ESS.