Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2846443 A1 2013/02/28

(21) 2 846 443

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2012/08/27
(87) Date publication PCT/PCT Publication Date: 2013/02/28
(85) Entrée phase nationale/National Entry: 2014/02/24
(86) N° demande PCT/PCT Application No.: US 2012/052554
(87) N° publication PCT/PCT Publication No.: 2013/029048
(30) Priorité/Priority: 2011/08/25 (US61/527,406)

(51) Cl.Int./Int.Cl. *G06F 17/21* (2006.01)

(71) Demandeur/Applicant:
DOCUSIGN, INC., US

(72) Inventeurs/Inventors:
GONSER, THOMAS H., US;
PETERSON, DONALD G., US

(74) Agent: SMART & BIGGAR

(54) Titre : SOLUTION MOBILE PERMETTANT DE SIGNER ET DE CONSERVER DES DOCUMENTS DE TIERS
(54) Title: MOBILE SOLUTION FOR SIGNING AND RETAINING THIRD-PARTY DOCUMENTS

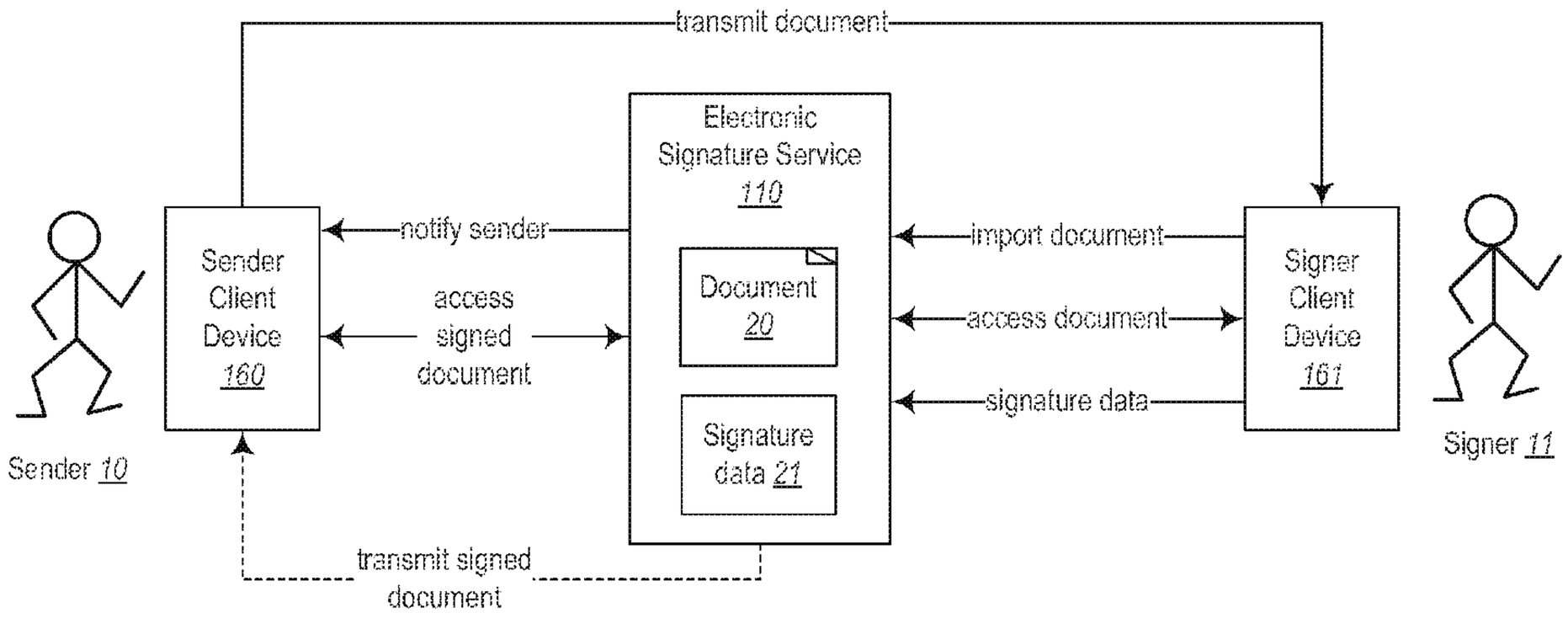

Fig. 1

(57) Abrégé/Abstract:
Techniques for signer-initiated electronic document signing via an electronic signature service using a mobile or other client device are described. Example embodiments provide an electronic signature service ("ESS") configured to facilitate the creation, storage, and management of documents and corresponding electronic signatures. In some embodiments, when a signer user receives an electronic signature document on a mobile device, the signer may use a client module executing on the mobile device to import the document into the ESS. Once the document is imported into the ESS, the signer can access, review, and sign the document at the ESS via the mobile device. After signing the document, the signer can use the mobile device to cause the ESS to provide the signed document to one or more recipients.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 February 2013 (28.02.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/029048 A1

(51) **International Patent Classification**:
G06F 17/21 (2006.01)

(21) **International Application Number**:
PCT/US2012/052554

(22) **International Filing Date**:
27 August 2012 (27.08.2012)

(25) **Filing Language**: English

(26) **Publication Language**: English

(30) **Priority Data**:
61/527,406 25 August 2011 (25.08.2011) US

(71) **Applicant** *(for all designated States except US)*: **DOCUSIGN, INC.** [US/US]; 1301 Second Avenue, Suite 2000, Seattle, WA 98101 (US).

(72) **Inventors; and**
(75) **Inventors/Applicants** *(for US only)*: **GONSER, Thomas, H.**; 3447 119th Avenue Ne, Bellevue, WA 98005 (US). **PETERSON, Donald, G.**; 6148 133rd Avenue Ne, Kirkland, WA 98033 (US).

(74) **Agent**: **LOWE, David, A.**; Lowe Graham Jones PLLC, 701 Fifth Avenue, Suite 4800, Seattle, WA 98104 (US).

(81) **Designated States** *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) **Designated States** *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

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

(54) Title: MOBILE SOLUTION FOR SIGNING AND RETAINING THIRD-PARTY DOCUMENTS

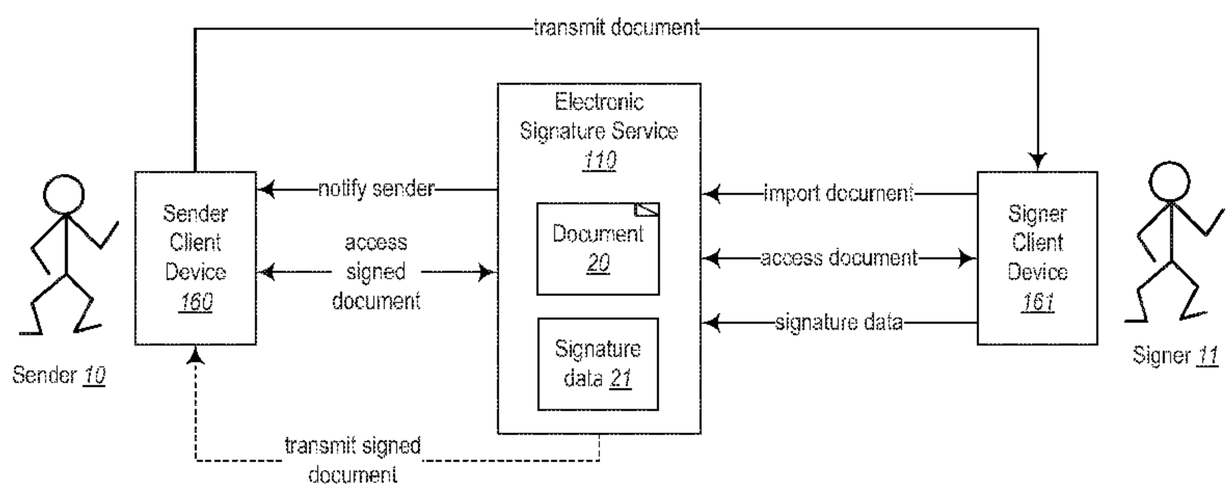

Fig. 1

(57) Abstract: Techniques for signer-initiated electronic document signing via an electronic signature service using a mobile or other client device are described. Example embodiments provide an electronic signature service ("ESS") configured to facilitate the creation, storage, and management of documents and corresponding electronic signatures. In some embodiments, when a signer user receives an electronic signature document on a mobile device, the signer may use a client module executing on the mobile device to import the document into the ESS. Once the document is imported into the ESS, the signer can access, review, and sign the document at the ESS via the mobile device. After signing the document, the signer can use the mobile device to cause the ESS to provide the signed document to one or more recipients.

WO 2013/029048 A1

MOBILE SOLUTION FOR SIGNING AND RETAINING THIRD-PARTY DOCUMENTS

PRIORITY CLAIM

[0001] This application claims the benefit of U.S. Provisional Application Serial No. 61/527,406 filed August 25, 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 to facilitate signer-initiated electronic document signing via an electronic signature service using a mobile or other client device.

BACKGROUND

[0003] One existing approach to electronic signatures provides an electronic signature "stamping" application for a mobile device. The signature application allows a user to open a document sent to them for signing and "stamp" a signature or other data into the document and return this by email. This approach suffers from a number of drawbacks. As one example, it only works with specific software applications for mobile devices, and the signing process is performed entirely in software on the mobile device. As such, the document must be manually moved from the email message into the device, manipulated, and then returned back to the device for email delivery. Also, to produce such an application for multiple devices or platforms requires that a largely redundant application be built for every platform, and then only for those platforms that have enough capability to actually

manipulate PDFs. Not all platforms or devices can actually handle tasks like conversion of files, presentation of files, managing signature capture and placement and security. The inability of mobile devices to universally perform all such required functions severely limits the expansion of electronic signature services, particularly in the mobile device context.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] Preferred and alternative examples of the present invention are described in detail below with reference to the following drawings:

[0005] FIGURE 1 illustrates a block diagram of an example embodiment of an electronic signature service;

[0006] FIGURES 2A-2D illustrate user interface screens according to example embodiments;

[0007] FIGURE 3 is a flow diagram of an example electronic signature client process; and

[0008] FIGURE 4 is a block diagram of a computing system for implementing an electronic signature service according to an example embodiment.

DETAILED DESCRIPTION

[0009] Embodiments described herein provide enhanced computer- and network-based methods and systems for mobile and other client devices to facilitate electronic document signing. Example embodiments provide an electronic signature service ("ESS") configured to facilitate the creation, storage, and management of documents and corresponding electronic signatures. Using the techniques described herein, a first user (a "sender") can transmit a document to be signed ("a signature document") to a mobile device

of a second user (a "signer"). Then, using a browser or other client module executing on the mobile device, the signer can import the document into the ESS. Once the document is imported into the ESS, the signer can access, review, and sign the document via the mobile device. After signing the document, the signer can use the mobile device to cause the ESS to provide the signed document to one or more recipients.

[0010] Some embodiments use a hybrid approach that leverages not only local software on a mobile device, but also use Internet cloud services that provide a consistent experience across all types of devices and platforms. In some implementations, minimal processing takes place locally on the mobile device, while the majority of the work performed (*e.g.*, securing the document, converting the files, managing the signing, and returning the file via email directly through the web, or via fax) is handled on a Web service application or in a browser on the mobile device, and is not reliant upon the local device/platform facilities (or lack thereof). Thus, such embodiments may provide access to electronic signature services to devices and platforms that do not include specific security or document conversion or manipulation (e.g., PDF conversion and manipulation) software.

[0011] 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 11 to facilitate an electronic signing of a signature document.

[0012] In the illustrated scenario, the sender 10 operates a sender client device 160 in order to transmit an electronic document (e.g., a contract or agreement) to a signer client device 161 operated by the signer 11. For example, the sender 10 may send an email with a

signature document included as an attachment to the email. The transmitted document may be in any format, such as PDF, Microsoft Word, HTML, text, or the like. Typically, the signer client device 161 is a mobile device, such as a smart phone, tablet computer, personal digital assistant, or the like. However, the techniques may be equally applied in other contexts and/or to other types of computing devices, including desktop computers, kiosk systems, and the like. In particular, some embodiments provide a module (e.g., plug-in, widget, extension) configured to perform some of the described techniques in the context of a desktop email client (e.g., Outlook), a hosted email service (*e.g.*, Google Mail, Yahoo! Mail, Hotmail), or other application. In addition, the techniques may generally be deployed (*e.g.*, as a signature module) in the context of any Web-based information or e-commerce service that has a need to obtain an electronic signature from a user (*e.g.*, to obtain assent to terms and conditions, to enter into purchase/sale agreements, etc.).

[0013] The signer 11 can then use client logic executing on the signer client device 161 to import the document into the ESS 110. For example, when the signer 11 uses an email client (on a mobile or other type of client device) to read an email that includes the signature document, the signer 11 can select a user interface control (*e.g.*, button, menu option, widget) of the email client to initiate an import of the signature document into the ESS 110. The document is then transmitted from the signer client device 161 to the ESS 110, where it is possibly converted and stored as document 20. Converting the document may include converting the document into a standard or preferred format for storage within the ESS 110. For example, if the original document was in Microsoft Word or HTML format, it may be converted into PDF by the ESS 110.

[0014] Once the document is imported into the ESS 110 and securely stored as document 20, the signer 11 can use the client device 161 to interact with the ESS 110 and perform various electronic signature-related operations. For example, the signer 11 can access and review the document by presenting and browsing the document using a browser or other client logic executing on the client device 161. As another example, the signer 11 can input data (*e.g.*, telephone number, address) into form fields or other input elements of the signature document 20. Once the signer 11 has reviewed and/or modified the document to his satisfaction, he can provide signature data which is then securely stored by the ESS 110 as signature data 21 in association with the document 20.

[0015] Once the signer 11 has signed the document 20, the signer 11 can cause the ESS to provide the signed document 20 a recipient. For example, the signer 11 may return the signed document to the sender 10 or some other recipient. Different approaches to providing signed documents are contemplated. In the illustrated embodiment, the signer 11 can cause the ESS 110 to notify the sender 10, such as by causing the ESS 110 to transmit (*e.g.*, in an email) a URL, link, or other identifier of the document 20 to the sender client device 160. The sender 10 can then use a browser or other client logic executing on the sender client device 160 to access the signed document on the ESS 110. Such an approach may be advantageous for sensitive documents which may preferably not be transmitted within an email or via some other possibly insecure transmission facility. In other embodiments, the ESS 110 can transmit the signed document 20 via an email, fax, or other transmission mechanism.

[0016] The ESS 110 may provide other or additional functions. For example, the ESS 110 may provide or facilitate intelligent form-filling operations. In one embodiment,

when the signer 11 repeatedly uses the ESS 110 to electronically sign documents, the ESS 110 tracks form data (*e.g.*, names, addresses, telephone numbers) provided by the signer 11, such that forms within signature documents can be automatically populated with data elements, thereby increasing the efficiency of the signature process.

[0017] In some embodiments, all or most of the above functions can be performed with a lightweight client (*e.g.*, a Web browser) executing on the client device 161, such that no or minimal special purpose software need be installed on the client device 161 to perform or access the full spectrum of signature services provided by the ESS 110. In this manner, described techniques overcome many of the limitations of known approaches to facilitating electronic signatures on mobile devices. For example, in a known approach, a client must install a special purpose signature application (a "signature app") on a mobile phone to attach electronic signatures to documents. Unfortunately, this application is distinct from the email client on the mobile phone, such that the user must manually move a received document into the signature app, attach a signature, move the signed document back to the email client, and then transmit the signed document to a recipient. Such processing is inefficient, cumbersome, and not user-friendly. Moreover, many signature apps do not include features such as document conversion, so they are unable to attach signatures to various common document formats. Furthermore, the diversity of mobile phone platforms (*e.g.*, iPhone, Android, Blackberry) means developing and supporting distinct applications for each platform. The described techniques, on the other hand, are largely platform independent, as the core functionality is provided by the ESS 110, but accessed from diverse clients using standard Web browsers.

[0018] FIGURES 2A-2D illustrate user interface screens according to example embodiments. FIGURE 2A illustrates a home screen 200 presented by a client device. The screen 200 may be provided by a mobile client device, such as a smart phone or tablet computer. In other embodiments, the screen 200 may be part of a file chooser/browser or desktop computing system. The screen 200 displays files and other data items managed by or stored on the client device. In the illustrated example, the screen 200 includes icons 201-203, respectively representing a first, second, and third file/document. The first document is a text document (*e.g.*, a Microsoft Word file). The document is an image file (*e.g.*, a JPG file). The third document is a PDF file.

[0019] The screen 200 also includes a menu control 204. The menu control 204 is displayed in response to a user selection (*e.g.*, tap, touch, mouse click) of icon 203. The menu control 204 presents commands or functions that may be performed with respect to the document represented by icon 203. One of the options is "Sign." When the Sign option is selected by the user, the illustrated embodiment will initiate a signature process as described herein, including by importing the document (of file3.pdf) into the ESS 110 and allowing the user to review and sign the document. An example screen configured to facilitate signature of the document is described with respect to FIGURE 2C, below.

[0020] FIGURE 2B illustrates a message screen 210 provided by an email client. The message screen 210 is configured to present a received email message 215 and provide access to various email functions, grouped into a tab menu 211. The tab menu 211 includes various function tabs, including a Sign tab that provides controls for electronically signing an attachment to the displayed email message 215.

[0021] In the illustrated example, the email message 215 includes an attachment (form.pdf) that is to be signed by the recipient of the message. To sign the attachment, the recipient user first selects the Sign tab. The Sign tab includes buttons 212-214. Button 212, when selected by the user, causes the attachment to be imported into the ESS 110 and invokes a signature process. Button 213 provides help documentation for new and returning users. Button 214 is configured to log the user out of the ESS 110.

[0022] The signature-related functionality described with respect to FIGURES 2A and 2B may be provided in various ways. In one embodiment, a plug-in or other code module is installed or otherwise added to the operating system, file manager, mail client, Web browser, or other software of the client device. Upon installation, a respective user interface (*e.g.*, menu control 204, tab menu 211) is modified to include controls (*e.g.*, the Sign option of menu control 204, the Sign tab or button 212 of tab menu 211) that are configured to invoke signature functions as described herein.

[0023] FIGURE 2C illustrates a signature screen 220 provided by a Web browser. The signature screen 220 is presented in response to an indication that a user desires to sign a document. For example, the screen 220 may be presented automatically in response to a user selection of the Sign option of menu control 204 (FIGURE 2A) or the Sign button 212 (FIGURE 2B). The signature screen 220 is presented within a Web browser and provides access to functionality of the ESS 110 for signing an electronic signature document. By performing signatures via a Web browser interface, no special electronic signature software need be installed on the user's client device.

[0024] The signature screen 220 displays a signature document 223 and includes a menu bar 221. The signature document 223 may be a copy or other representation of an attachment or other document imported by the user, as discussed above. The menu bar 221 includes an Add control, a Finish control, and a More Options control. The Add control, when selected, displays a menu 222 of signature elements. The signature elements include a signature, signer initials, signer name, signer company, signer title, date signed, text, and checkbox. By selecting one of the signature elements, the user/signer can insert (*e.g.*, drag and drop) the corresponding element into the signature document 223. For example, by selecting the "Signature" signature element, the user can insert or associate his signature into the document 223. By selecting the "My Name" signature element, the user can insert his printed name into the document 223.

[0025] When the user has reviewed and signed the document 223, the user selects the Finish control of the menu 221. The Finish control causes the now modified document 223 to be securely stored by the ESS 110. The Finish control may also provide options or otherwise access functions for providing the signed document 223 to one or more recipients. For example, the Finish control may automatically invoke an email client on the signer's client device, as described next with respect to FIGURE 2D.

[0026] FIGURE 2D illustrates a message composition screen 230 provided by an email client. The email client may in some embodiments be automatically invoked upon the conclusion of the signature process described with respect to FIGURE 2C, above. The message composition screen 230 includes an automatically generated email message 231. The message 231 includes header fields (*e.g.*, to, from, subject) that may be automatically

populated, based on information about the user's past actions or context. For example, if the user invoked the signature process from within the message screen 210 of FIGURE 2B, the email address of the sender of the message 215 (john@firsthost) may be automatically transmitted to the ESS (along with the attachment to be signed). After signature, the email address of the original sender may be provided back to the email client for inclusion as the recipient of the message 231. A similar technique may be used to automatically populate other fields, such as the subject line of the message 231. The message 231 also includes marketing text ("I used DocuSignIt … Visit DocuSign …") that describes the ESS 110 and encourages the message recipient to access and/or sign up for an account with the ESS 110.

[0027] In other embodiments, the message 231 does not include the signed document as an attachment. Rather, the message 231 may include a link or other identifier that can be used by the recipient to access the signed document at the ESS 110 or some other location.

[0028] FIGURE 3 is a flow diagram of an example electronic signature client process. The illustrated process may be performed by, for example, logic executing on the signer client device 161.

[0029] The process begins at block 302, where it receives an electronic signature document. As noted, the client device 161 may receive the document in various ways, such as by receiving an email, downloading a file (*e.g.*, from a Web site), or the like.

[0030] At block 304, the process causes the received electronic signature document to be stored at a remote electronic signature service. The client device 161 may include logic that uploads, imports, or otherwise transmits the document to the electronic signature service

in response to a user input. For example, an email client may include a plug-in or other module with which the user of the client device 161 can import the document to the electronic signature service for storage, review, signature, and/or distribution.

[0031] At block 306, the process provides access to the electronic signature document stored at the remote electronic signature service. Providing access may include automatically launching or invoking a Web browser or other client module that can be used to access, review, and sign the document at the remote electronic signature service. Using the Web browser or other client module, the user may review, modify, and sign the document.

[0032] At block 308, the process causes an electronic signature to be stored at the electronic signature service in association with the electronic signature document. Typically, the client module (*e.g.*, Web browser) invoked at block 306, above will be operated by the user to then sign the document. Once the user signs the document, the electronic signature service will securely store the signature in association with the document.

[0033] 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. Note that the techniques described for implementing the electronic signature service 110 may similarly be applied to implementing client logic (*e.g.*, a plug-in) for importing and initiating electronic signature processes on a client device.

[0034] 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.

[0035] 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 facilitate mobile electronic signature processes 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.

[0036] The electronic signature service 110 includes a service 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.

[0037] 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 and/or a signer client device 161. In one embodiment, a signer operating signer client device 161 imports (*e.g.*, transmits, uploads, sends) a document to be electronically signed into 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. The 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. After signing the document, the signer using signer client device 161 can cause the ESS 110 to provide the signed document to one or more recipients, such as via email, fax, or other mechanism.

[0038] The service manager 111 may perform other or additional functions, such as intelligent form filling as discussed above. Also, the service manager 111 may provide code modules that can be installed on the signer client device 161 and that are configured to integrate the signer client device 161 with the ESS 110. For example, a code module may be installed on the signer client device 161 and extend the functionality of an email client by adding a control (*e.g.*, button, menu item, widget) that is configured to import, in response to selection or activation by a user, a received documents into the ESS 110.

[0039] 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, review and modify documents, transmit or otherwise provide signed documents to recipients, 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.

[0040] 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 hosted email service executing on the system 165 may provide access to the electronic signature functionality of the ESS 110 via the API 113. As another example, an e-commerce site (*e.g.*, online store) executing on the system 165 may provide access to the electronic

signature functionality of the ESS 110 via the API 113, such as by providing a signature control/widget configured, when selected by a user, to initiate an electronic signature process as described herein.

[0041] 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, tracked form entries, 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.

[0042] 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.

[0043] 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).

[0044] 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.

[0045] In addition, programming interfaces to the data stored as part of the electronic signature service 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.

[0046] 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.

[0047] 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 components and/or data structures may be stored on tangible, non-transitory storage mediums. 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.

[0048] 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.

[0049] All of the above-cited references, including Appendixes A and B, are incorporated herein by reference in their entirety. Where a definition or use of a term in an incorporated reference is inconsistent or contrary to the definition of that term provided herein, the definition of that term provided herein governs and the definition of that term in the reference does not apply.

[0050] 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 facilitating electronic signatures on a client device operated by a signer, comprising in the client device:

receiving an electronic signature document;

in response to an input received from the signer, causing the received electronic signature document to be stored at a remote electronic signature service;

providing access to the electronic signature document stored at the remote electronic signature service; and

causing an electronic signature of the signer to be stored in association with the electronic signature document stored at the remote electronic signature service.

2. The method of claim 1, further comprising causing the remote electronic signature service to provide the stored electronic signature document to a recipient.

3. The method of claim 2, wherein causing the remote electronic signature service to provide the stored electronic signature document to a recipient includes transmitting from the remote electronic signature service to the recipient a copy of the stored electronic signature document as an attachment to an email.

4. The method of claim 2, wherein causing the remote electronic signature service to provide the stored electronic signature document to a recipient includes transmitting from the remote electronic signature service to the recipient a copy of the stored electronic signature document as a fax.

5. The method of claim 2, wherein causing the remote electronic signature service to provide the stored electronic signature document to a recipient includes transmitting from the remote electronic signature service to the recipient an email including an identifier of the

stored electronic signature document, the identifier configured to facilitate access to the stored electronic signature document at the remote electronic signature service.

6. The method of claim 1, wherein the client device is a mobile device and includes an email client that is configured to, in response to the input received from the signer, transmit the electronic signature document to the remote electronic signature service.

7. The method of claim 1, further comprising using a Web browser executing on the client device to access the electronic signature document stored at the remote electronic signature service and to cause the electronic signature of the signer to be stored in association with the electronic signature document.

8. The method of claim 1, further comprising automatically populating form fields in the electronic signature document based on prior form entries made by the signer.

9. The method of claim 1, further comprising installing a code module on the client device, the code module configured to transparently import documents obtained from an email client of the client device into the remote electronic signature service.

10. A non-transitory computer-readable medium having contents that, when executed by a client device, facilitate electronic signatures via the client device by performing a method comprising in the client device:

receiving an electronic signature document;

in response to an input received from the signer, causing the received electronic signature document to be stored at a remote electronic signature service;

providing access to the electronic signature document stored at the remote electronic signature service; and

causing an electronic signature of the signer to be stored in association with the electronic signature document stored at the remote electronic signature service.

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

12. The computer-readable medium of claim 10, wherein providing access to the electronic signature document includes, after the electronic signature document is stored at the remote electronic signature service, automatically causing a Web browser of the client device to access an electronic signature service application hosted by the remote electronic signature service, the application configured to facilitate review, modification, and signature by the signer of the electronic signature document.

13. The computer-readable medium of claim 12, further comprising in response to the storage of the electronic signature of signer, automatically causing an email client of the client device to prepare an outgoing email message that includes an attached file that represents electronic signature document including the electronic signature of the signer.

14. The computer-readable medium of claim 13, wherein receiving the electronic signature document includes receiving an email message that includes the electronic signature document, and further comprising:

determining an email address based on a source address field of the received email message; and

including the email address in a destination address field of the outgoing email message.

15. A computing system configured to facilitate electronic signatures, comprising:

a client device having a processor and memory; and

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

receive an electronic signature document;

in response to an input received from the signer, cause the received electronic signature document to be stored at a remote electronic signature service;

provide access to the electronic signature document stored at the remote electronic signature service; and

cause an electronic signature of the signer to be stored in association with the electronic signature document stored at the remote electronic signature service.

16. The computing system of claim 15, wherein the module includes software instructions for execution in the memory of the computing system.

17. The computing system of claim 15, further comprising an electronic signature service that is remote from the client device and that is configured to perform electronic signature management functions and to provide access to the electronic signature management functions via a Web browser executing on the client device.

18. The computing system of claim 15, wherein the client device is a smart phone or a tablet computer.

19. The computing system of claim 15, wherein the client device does not include PDF conversion or manipulation software.

20. The computing system of claim 15, wherein the module is configured to, after storage of the electronic signature of the signer, transmit a signed copy of the electronic signature document via email to an originator of the electronic signature document.

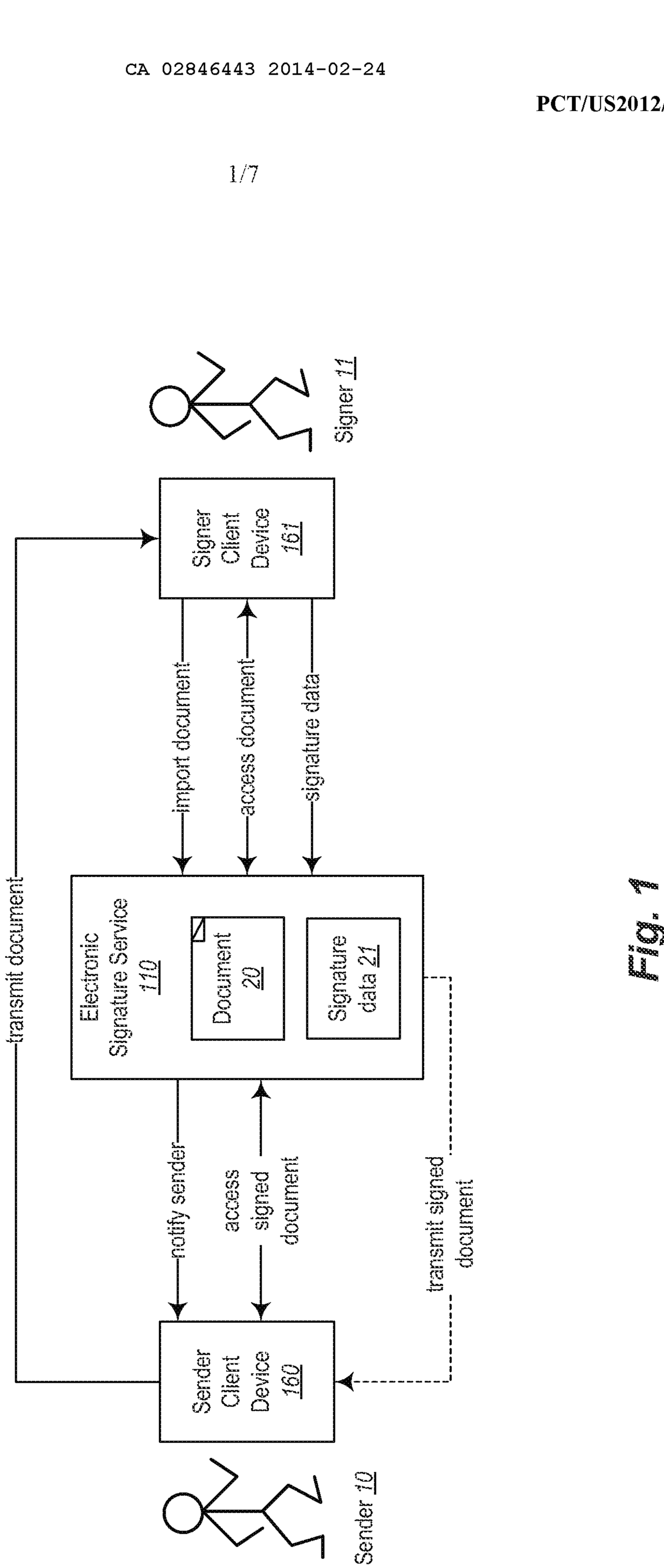
Signer 11
Signer Client Device 161
import document
access document
signature data
transmit document
Electronic Signature Service 110
Document 20
Signature data 21
notify sender
access signed document
transmit signed document
Sender Client Device 160
Sender 10

Fig. 1

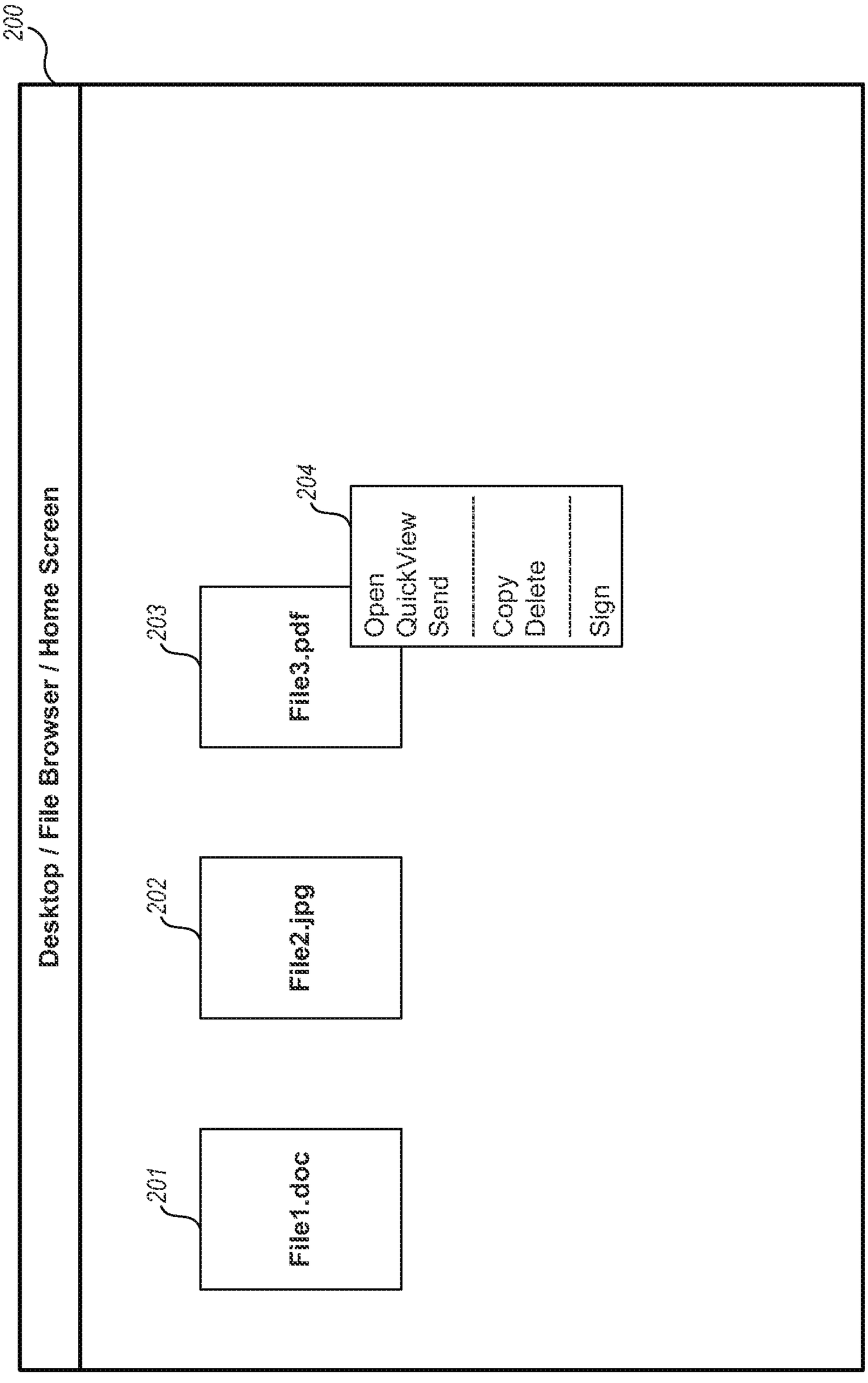
200
Desktop / File Browser / Home Screen
201
File1.doc
202
File2.jpg
203
File3.pdf
204
Open
QuickView
Send
Copy
Delete
Sign

Fig. 2A

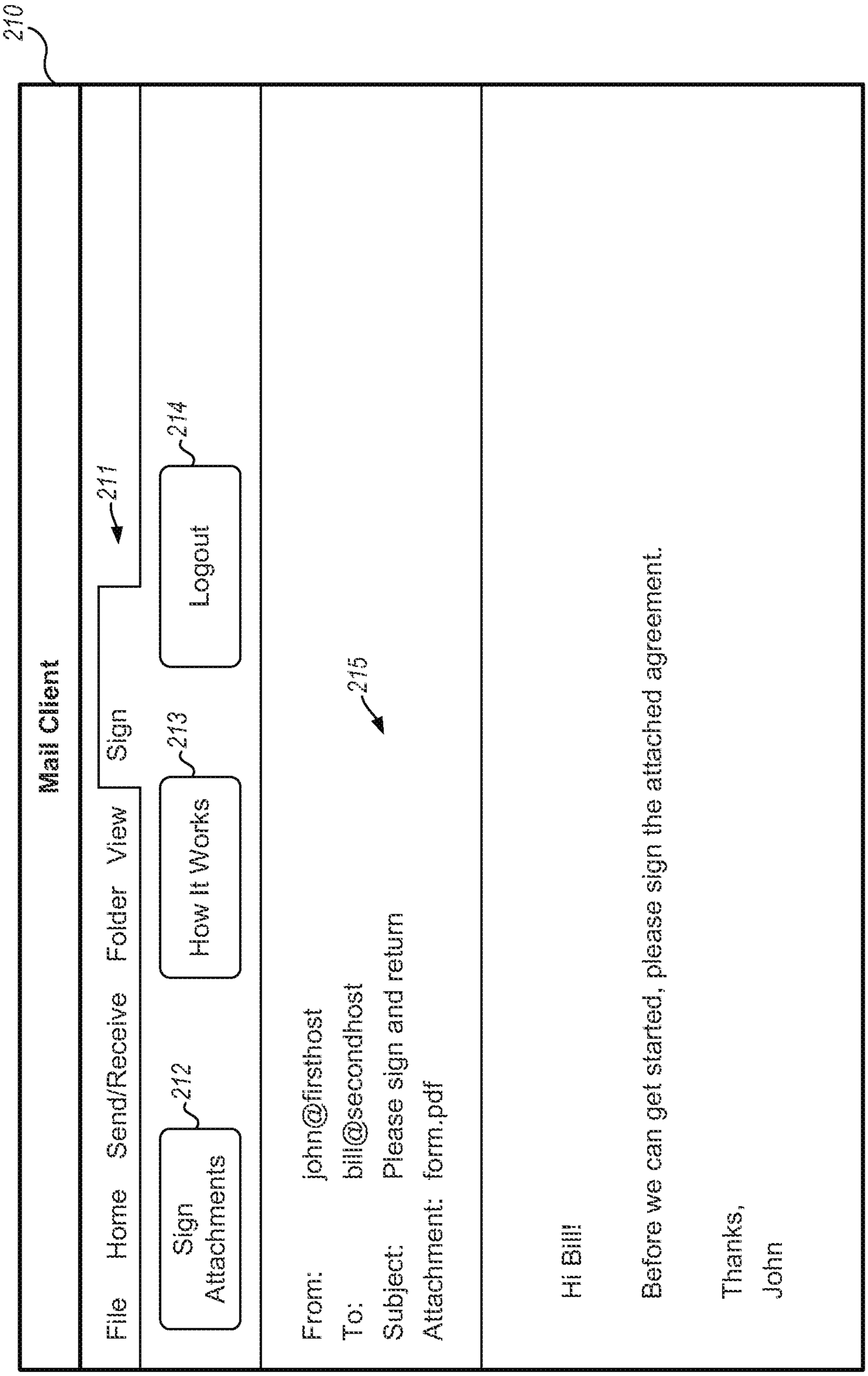
210
Mail Client
File Home Send/Receive Folder View Sign
Sign Attachments
212
How It Works
213
214
Logout
211
From: john@firsthost
To: bill@secondhost
Subject: Please sign and return
Attachment: form.pdf
215
Hi Bill!
Before we can get started, please sign the attached agreement.
Thanks,
John

Fig. 2B

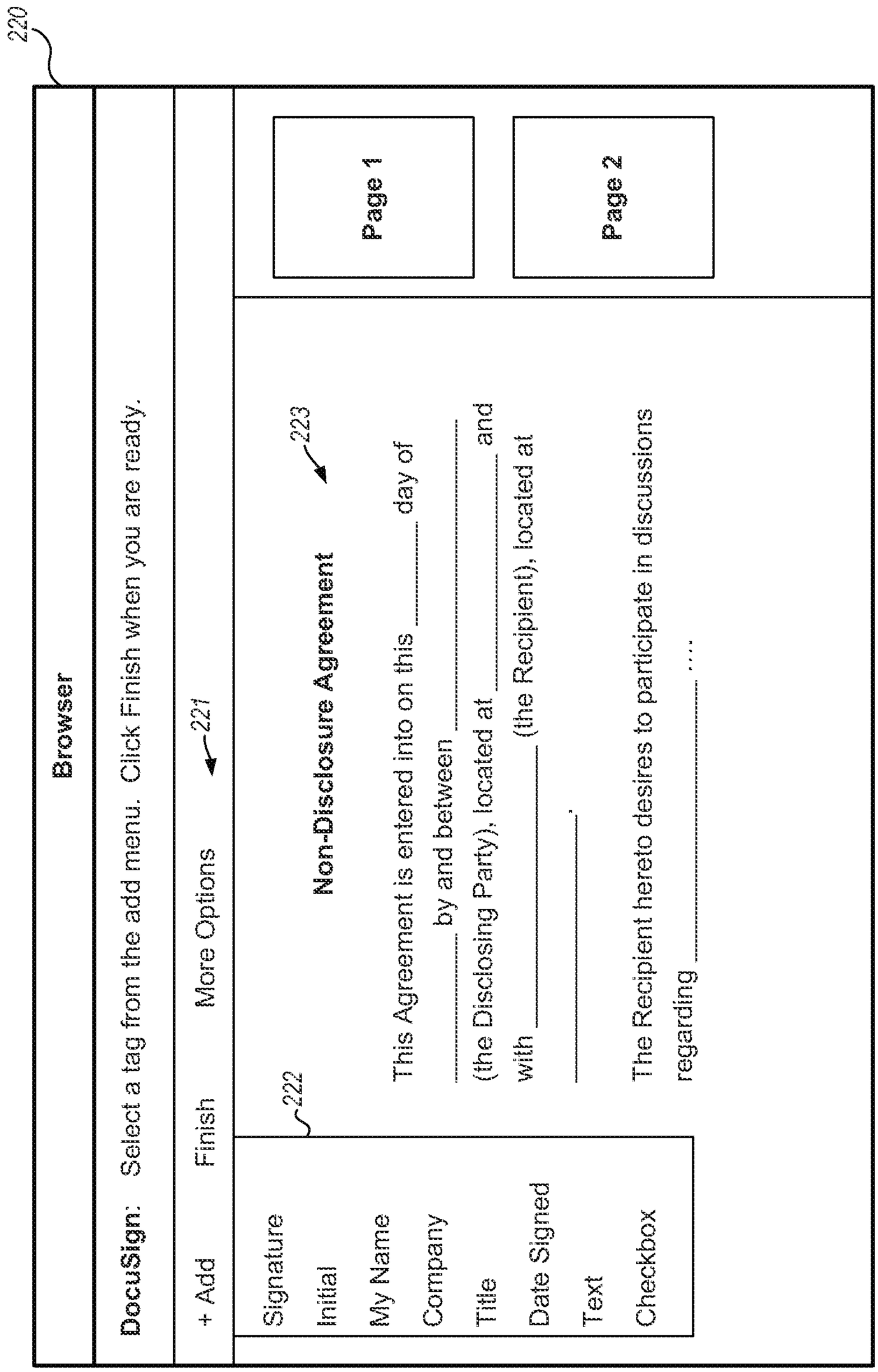
220
Browser
Select a tag from the add menu. Click Finish when you are ready.
DocuSign:
+ Add
Finish
Signature
Initial
My Name
Company
Title
Date Signed
Text
Checkbox
222
223
Page 1
Page 2
Non-Disclosure Agreement
This Agreement is entered into on this ____ day of
_____ by and between _____ and
(the Disclosing Party), located at _____
with _____ (the Recipient), located at
_____.
The Recipient hereto desires to participate in discussions
regarding _____ ....
More Options
221

Fig. 2C

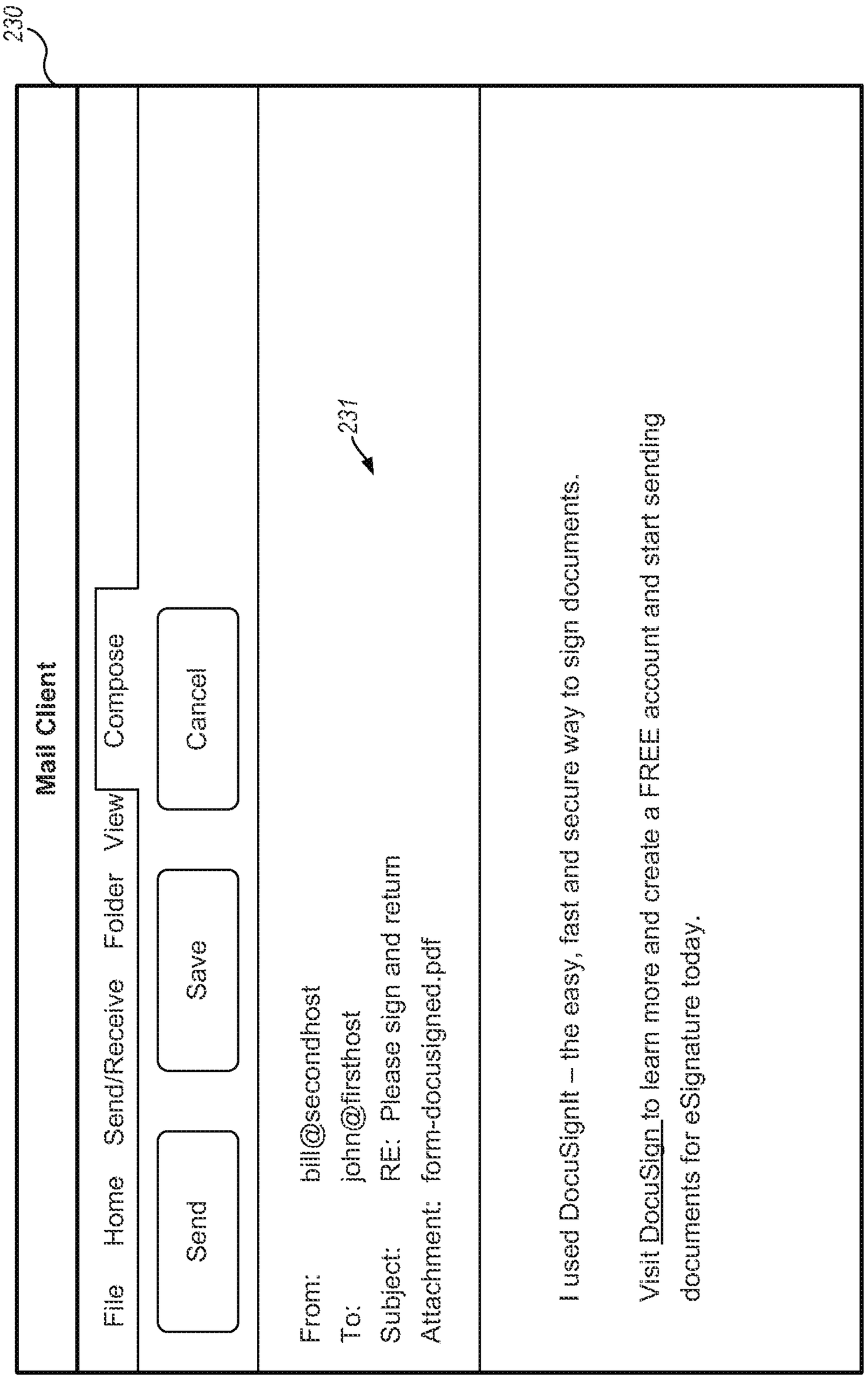
230
231
Mail Client
File Home Send/Receive Folder View Compose
Send
Save
Cancel
From: bill@secondhost
To: john@firsthost
Subject: RE: Please sign and return
Attachment: form-docusigned.pdf
I used DocuSignIt – the easy, fast and secure way to sign documents.
Visit DocuSign to learn more and create a FREE account and start sending documents for eSignature today.

Fig. 2D

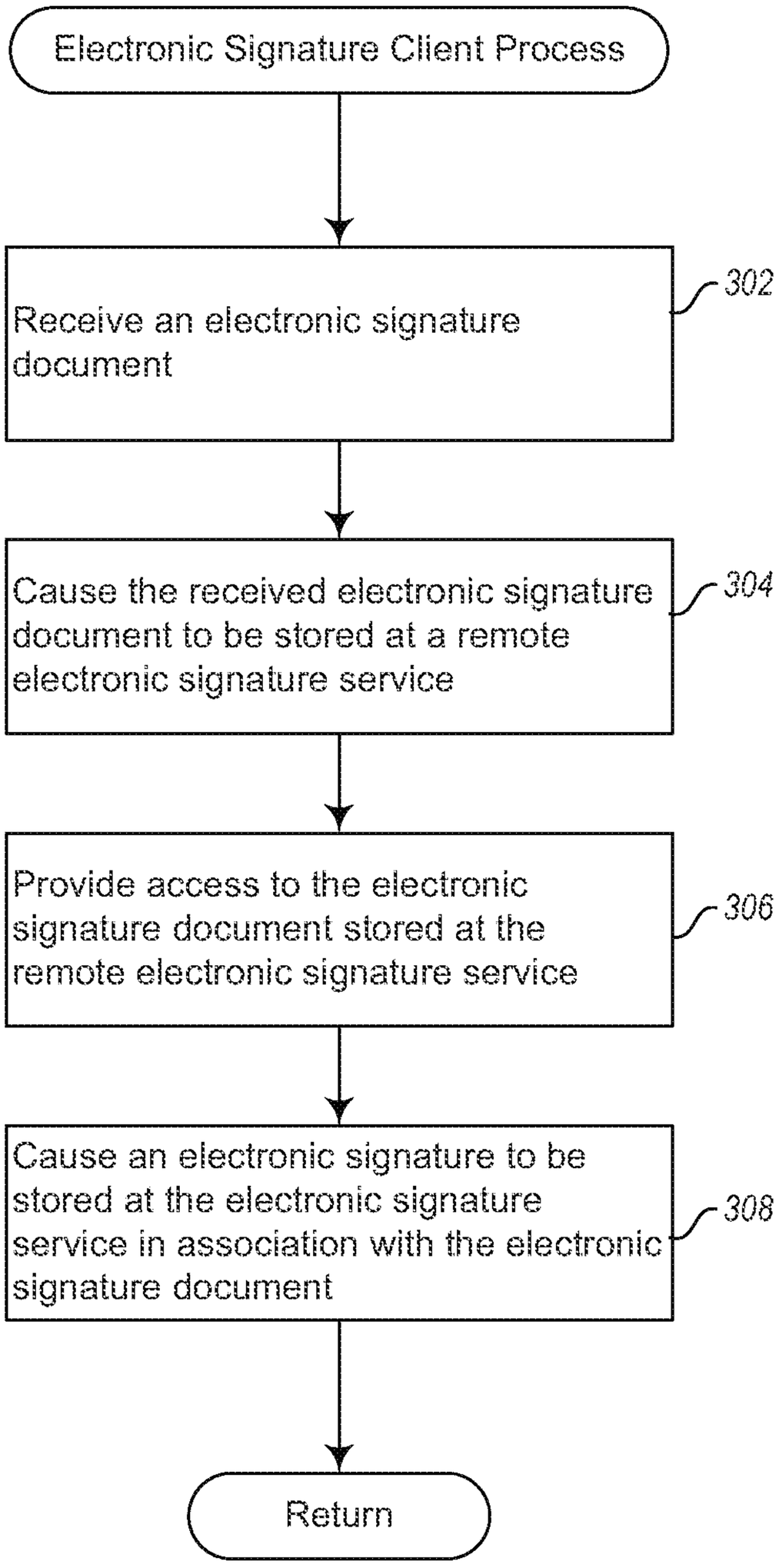
Electronic Signature Client Process
Receive an electronic signature document
302
Cause the received electronic signature document to be stored at a remote electronic signature service
304
Provide access to the electronic signature document stored at the remote electronic signature service
306
Cause an electronic signature to be stored at the electronic signature service in association with the electronic signature document
308
Return

Fig. 3

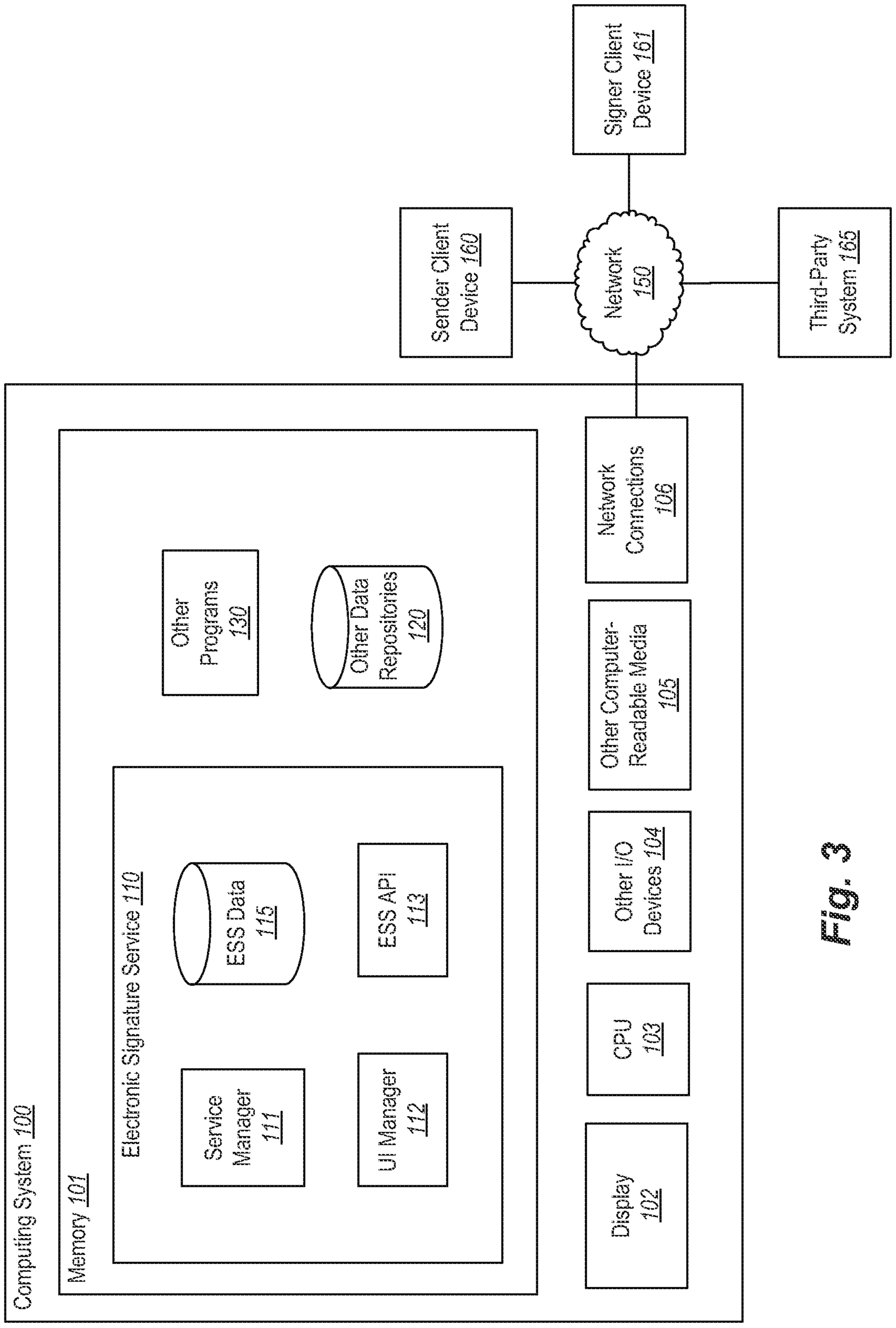
Signer Client Device 161
Sender Client Device 160
Network 150
Third-Party System 165
Network Connections 106
Other Computer-Readable Media 105
CPU 103
Other I/O Devices 104
Display 102
Computing System 100
Memory 101
Electronic Signature Service 110
Other Programs 130
Other Data Repositories 120
ESS Data 115
ESS API 113
Service Manager 111
UI Manager 112

Fig. 3

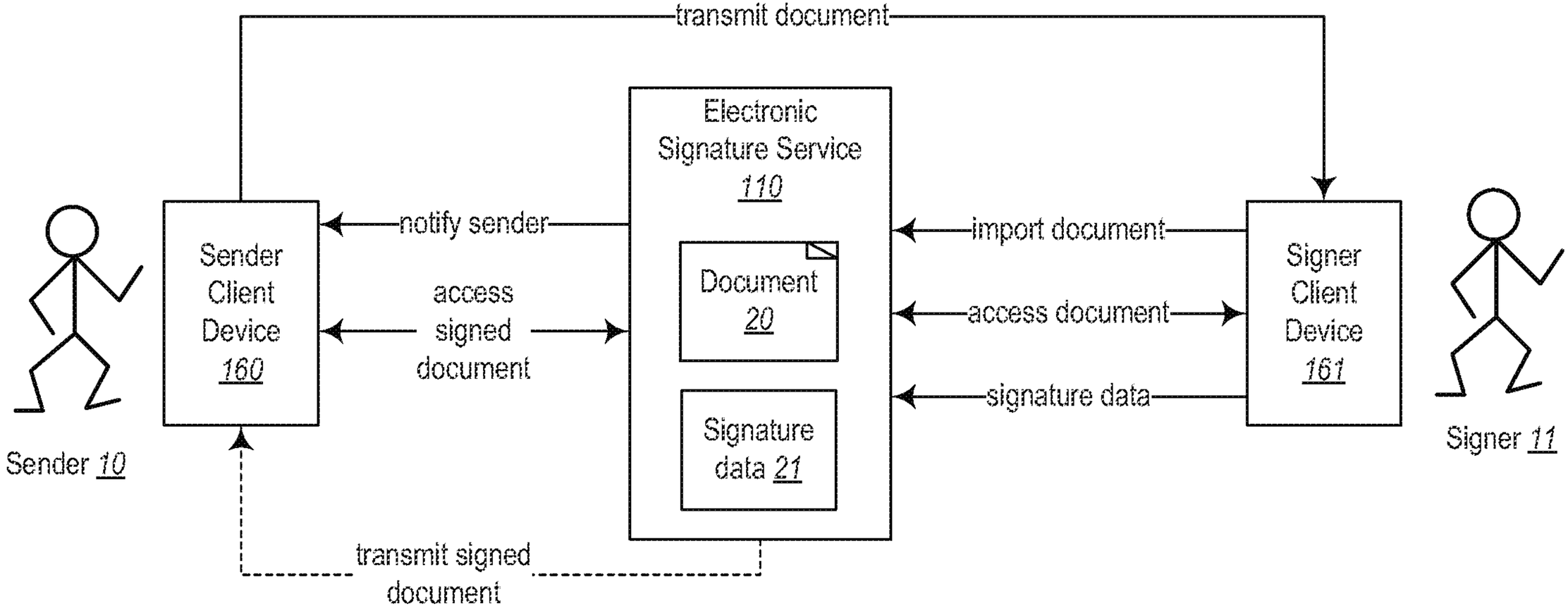
transmit document
Electronic
Signature Service
110
notify sender
access
signed
document
Document
20
Signature
data 21
import document
access document
signature data
Sender
Client
Device
160
Signer
Client
Device
161
Sender 10
Signer 11
transmit signed
document

Fig. 1