

SYSTEMS, METHODS, AND MEDIA FOR GENERATING DOCUMENTS CONTAINING CONFIDENTIAL INFORMATION

Cross Reference To Related Applications

[0001] This application claims the benefit of United States Patent Application No. 17/356,097, filed June 23, 2021, the benefit of United States Patent Application No. 17/356,104, filed June 23, 2021, the benefit of United States Patent Application No. 17/356,109, filed June 23, 2021, and the benefit of United States Patent Application No. 17/567,640, filed January 3, 2022, each of which is hereby incorporated by reference herein in its entirety.

Background

[0002] Confidential information, such as personally identifiable information (PII), medical information (e.g., protected health information regulated under the United States' Health Insurance Portability and Accountability Act (HIPAA)), and customer information (e.g., information of customers of financial services firms and law firms), needs to be secured against disclosure to parties who should not have that information. In many instances, when an organization (e.g., a company) is working with another party (e.g., a vendor) that generates documents related to confidential information, it is necessary to provide the confidential information to the other party. Unfortunately, providing the confidential information to the other party exposes the organization to risks that the confidential information will be stolen and/or misused, which could then expose the organization to liability (e.g., under the European Union's General Data Protection Regulation) and loss of revenue.

[0003] Accordingly, it is desirable to provide new mechanisms for generating documents containing confidential information.

Summary

[0004] In accordance with some embodiments, systems, methods, and media for generating documents containing confidential information are provided.

[0005] In some embodiments, systems for generating documents with confidential information are provided, the systems comprising: a memory; and a first collection of at least of one hardware processor coupled to the memory and configured to: receive from a user device a request for a first document with confidential information; generate a second document, that corresponds to the first document, with at least one token corresponding to the confidential information; transmit the second document to a second collection of at least one hardware processor in a high-trust network that is entitled to access the confidential information; receive from the second collection of at least one hardware processor in the high-trust network a uniform resource locator (URL) corresponding to the first document; and transmit the URL to the user device. In some of these embodiments, the user device is in the high trust network. In some of these embodiments, the second collection of at least one hardware processor in the high-trust network is in a server. In some of these embodiments, the first document is stored on the server. In some of these embodiments, the second collection of at least one hardware processor configured to: receive the second document from the first collection of at least one hardware processor; replace the at least one token in the second document to produce the first document; cause the first document to be stored; and transmit the URL to the first collection of at least one hardware processor. In some of these embodiments, the second collection of at least one hardware processor is further configured to serve the first document to the user device. In some of these embodiments, the user device is configured to: send the request for a first document to the first collection of at least one hardware processor; receive the URL; request the first

document using the URL; receive the first document; and cause the first document to be presented.

[0006] In some embodiments, methods for generating documents with confidential information are provided, the methods comprising: receiving from a user device a request for a first document with confidential information; generating a second document, that corresponds to the first document, with at least one token corresponding to the confidential information using a first collection of at least one hardware processor; transmitting the second document to a second collection of at least one hardware processor in a high-trust network that is entitled to access the confidential information using the first collection of at least one hardware processor; receiving from the second collection of at least one hardware processor in the high-trust network a uniform resource locator (URL) corresponding to the first document; and transmitting the URL to the user device. In some of these embodiments, the user device is in the high trust network. In some of these embodiments, the second collection of at least one hardware processor in the high-trust network is in a server. In some of these embodiments, the first document is stored on the server. In some of these embodiments, the second collection of at least one hardware processor configured to: receive the second document from the first collection of at least one hardware processor; replace the at least one token in the second document to produce the first document; cause the first document to be stored; and transmit the URL to the first collection of at least one hardware processor. In some of these embodiments, the second collection of at least one hardware processor is further configured to serve the first document to the user device. In some of these embodiments, the user device is configured to: send the request for a first document to the first collection of at least one hardware processor; receive the URL; request the first document using the URL; receive the first document; and cause the first document to be presented.

[0007] In some embodiments, non-transitory computer-readable media containing computer executable instructions that, when executed by a first collection of at least one hardware processor, cause the first collection of at least one hardware processor to perform a method for generating documents with confidential information are provided, the method comprising: receiving from a user device a request for a first document with confidential information; generating a second document, that corresponds to the first document, with at least one token corresponding to the confidential information; transmitting the second document to a second collection of at least one hardware processor in a high-trust network that is entitled to access the confidential information; receiving from the second collection of at least one hardware processor in the high-trust network a uniform resource locator (URL) corresponding to the first document; and transmitting the URL to the user device. In some of these embodiments, the user device is in the high trust network. In some of these embodiments, the second collection of at least one hardware processor in the high-trust network is in a server. In some of these embodiments, the first document is stored on the server. In some of these embodiments, the second collection of at least one hardware processor configured to: receive the second document from the first collection of at least one hardware processor; replace the at least one token in the second document to produce the first document; cause the first document to be stored; and transmit the URL to the first collection of at least one hardware processor. In some of these embodiments, the second collection of at least one hardware processor is further configured to serve the first document to the user device. In some of these embodiments, the user device is configured to: send the request for a first document to the first collection of at least one hardware processor; receive the URL; request the first document using the URL; receive the first document; and cause the first document to be presented.

[0008] In some embodiments, systems for generating documents with confidential information are provided, the systems comprising: a memory; and a first collection of at least of one hardware processor coupled to the memory and configured to: receive a first document from a second collection of at least one hardware processor; replace at least one token in the first document to produce a second document; cause the second document to be stored; and transmit a uniform resource locator (URL) corresponding to the second document to the second collection of at least one hardware processor. In some of these embodiments, the first collection of at least one hardware processor is further configured to serve the first document to a user device. In some of these embodiments, the user device is configured to: send a request for the first document to the first collection of at least one hardware processor; receive the URL; request the first document using the URL; receive the first document; and cause the first document to be presented. In some of these embodiments, the second collection of at least one hardware processor is configured to: generate the first document, that corresponds to the second document, with at least one token corresponding to confidential information; transmit the first document to the first collection of at least one hardware processor in a high-trust network that is entitled to access the confidential information; receive from the first collection of at least one hardware processor in the high-trust network a uniform resource locator (URL) corresponding to the second document; and transmit the URL to a user device. In some of these embodiments, the user device is in a high trust network. In some of these embodiments, the first collection of at least one hardware processor is in a server. In some of these embodiments, the second document is stored on the server.

[0009] In some embodiments, methods for generating documents with confidential information are provided, the methods comprising: receiving, using a first collection of at least one hardware processor, a first document from a second collection of at least one hardware

processor; replacing, using the first collection of at least one hardware processor, at least one token in the first document to produce a second document; causing the second document to be stored; and transmitting a uniform resource locator (URL) corresponding to the second document to the second collection of at least one hardware processor. In some of these embodiments, the methods further comprise serving the first document to a user device. In some of these embodiments, the user device is configured to: send a request for the first document to the first collection of at least one hardware processor; receive the URL; request the first document using the URL; receive the first document; and cause the first document to be presented. In some of these embodiments, the second collection of at least one hardware processor is configured to: generate the first document, that corresponds to the second document, with at least one token corresponding to confidential information; transmit the first document to the first collection of at least one hardware processor in a high-trust network that is entitled to access the confidential information; receive from the first collection of at least one hardware processor in the high-trust network a uniform resource locator (URL) corresponding to the second document; and transmit the URL to a user device. In some of these embodiments, the user device is in a high trust network. In some of these embodiments, the first collection of at least one hardware processor is in a server. In some of these embodiments, the second document is stored on the server.

[0010] In some embodiments, non-transitory computer-readable media containing computer executable instructions that, when executed by a first collection of at least one hardware processor, cause the first collection of at least one hardware processor to perform a method for generating documents with confidential information are provided, the method comprising: receiving a first document from a second collection of at least one hardware processor; replacing at least one token in the first document to produce a second document; causing the second document to be stored; and transmitting a uniform resource locator (URL) corresponding to the

second document to the second collection of at least one hardware processor. In some of these embodiments, the method further comprises serving the first document to a user device. In some of these embodiments, the user device is configured to: send a request for the first document to the first collection of at least one hardware processor; receive the URL; request the first document using the URL; receive the first document; and cause the first document to be presented. In some of these embodiments, the second collection of at least one hardware processor is configured to: generate the first document, that corresponds to the second document, with at least one token corresponding to confidential information; transmit the first document to the first collection of at least one hardware processor in a high-trust network that is entitled to access the confidential information; receive from the first collection of at least one hardware processor in the high-trust network a uniform resource locator (URL) corresponding to the second document; and transmit the URL to a user device. In some of these embodiments, the user device is in a high trust network. In some of these embodiments, the first collection of at least one hardware processor is in a server. In some of these embodiments, the second document is stored on the server.

[0011] In some embodiments, systems for generating documents with confidential information are provided, the systems comprising: a user device configured to: send a request for a first document with confidential information to a first collection of at least one hardware processor in a low-trust network that is not entitled to access the confidential information; receive a uniform resource locator (URL) corresponding to the first document from the first collection of at least one hardware processor; request the first document using the URL from a second collection of at least one hardware processor in a high-trust network that is entitled to access the confidential information; receive the first document; and cause the first document to be presented. In some of these embodiments, the user device is in the high trust network. In

some of these embodiments, the second collection of at least one hardware processor in the high-trust network is in a server. In some of these embodiments, the first document is stored on the server. In some of these embodiments, the first collection of at least one hardware processor is configured to: receive from the user device the request for the first document; generate a second document, that corresponds to the first document, with at least one token corresponding to the confidential information; transmit the second document to the second collection of at least one hardware processor; receive from the second collection of at least one hardware processor a uniform resource locator (URL) corresponding to the first document; and transmit the URL to the user device. In some of these embodiments, the second collection of at least one hardware processor is configured to: receive the second document from the first collection of at least one hardware processor; replace the at least one token in the second document to produce the first document; cause the first document to be stored; and transmit the URL to the first collection of at least one hardware processor. In some of these embodiments, the second collection of at least one hardware processor is further configured to serve the first document to the user device.

[0012] In some embodiments, methods for generating documents with confidential information are provided, the methods comprising: sending, from a user device, a request for a first document with confidential information to a first collection of at least one hardware processor in a low-trust network that is not entitled to access the confidential information; receive a uniform resource locator (URL) corresponding to the first document from the first collection of at least one hardware processor at the user device; request, from the user device, the first document using the URL from a second collection of at least one hardware processor in a high-trust network that is entitled to access the confidential information; receive the first document at the user device; and cause the first document to be presented. In some of these embodiments, the user device is in the high trust network. In some of these embodiments, the

second collection of at least one hardware processor in the high-trust network is in a server. In some of these embodiments, the first document is stored on the server. In some of these embodiments, the first collection of at least one hardware processor is configured to: receive from the user device the request for the first document; generate a second document, that corresponds to the first document, with at least one token corresponding to the confidential information; transmit the second document to the second collection of at least one hardware processor; receive from the second collection of at least one hardware processor a uniform resource locator (URL) corresponding to the first document; and transmit the URL to the user device. In some of these embodiments, the second collection of at least one hardware processor is configured to: receive the second document from the first collection of at least one hardware processor; replace the at least one token in the second document to produce the first document; cause the first document to be stored; and transmit the URL to the first collection of at least one hardware processor. In some of these embodiments, the second collection of at least one hardware processor is further configured to serve the first document to the user device.

[0013] In some embodiments, non-transitory computer-readable media containing computer executable instructions that, when executed by at least one processor in a user device, cause the at least one processor to perform a method for generating documents with confidential information are provided, the method comprising: sending a request for a first document with confidential information to a first collection of at least one hardware processor in a low-trust network that is not entitled to access the confidential information; receive a uniform resource locator (URL) corresponding to the first document from the first collection of at least one hardware processor; request the first document using the URL from a second collection of at least one hardware processor in a high-trust network that is entitled to access the confidential information; receive the first document; and cause the first document to be presented. In some of

these embodiments, the user device is in the high trust network. In some of these embodiments, the second collection of at least one hardware processor in the high-trust network is in a server. In some of these embodiments, the first document is stored on the server. In some of these embodiments, the first collection of at least one hardware processor is configured to: receive from the user device the request for the first document; generate a second document, that corresponds to the first document, with at least one token corresponding to the confidential information; transmit the second document to the second collection of at least one hardware processor; receive from the second collection of at least one hardware processor a uniform resource locator (URL) corresponding to the first document; and transmit the URL to the user device. In some of these embodiments, the second collection of at least one hardware processor is configured to: receive the second document from the first collection of at least one hardware processor; replace the at least one token in the second document to produce the first document; cause the first document to be stored; and transmit the URL to the first collection of at least one hardware processor. In some of these embodiments, the second collection of at least one hardware processor is further configured to serve the first document to the user device.

Brief Description of the Drawings

[0014] FIG. 1 is an example of a system for generating documents containing confidential information in accordance with some embodiments.

[0015] FIG. 2 is an example of hardware that can be used to implement some components of the system of FIG. 1 in accordance with some embodiments.

[0016] FIG. 3 is an example of a document containing tokens in place of confidential information in accordance with some embodiments.

[0017] FIG. 4 is an example of a document containing confidential information in accordance with some embodiments.

[0018] FIG. 5 is an example of an entity record and an anonymized entity record in accordance with some embodiments.

[0019] FIG. 6 is an example of an address record and an anonymized address record in accordance with some embodiments.

[0020] FIG. 7 is an example of an account record and an anonymized account record in accordance with some embodiments.

[0021] FIG. 8 is an example of a process for generating a document containing confidential information in accordance with some embodiments.

[0022] FIG. 9 is an example of process for synchronizing confidential information and tokens between a high-trust network and a low-trust network in accordance with some embodiments.

Detailed Description

[0023] In accordance with some embodiments, mechanisms (which can include systems, methods, and media) for generating documents containing confidential information are provided.

[0024] As described in more detail below, in some embodiments, in order to protect confidential information from theft and/or misuse, the confidential information can be stored in and accessed from a high-trust network. Devices in the high-trust network can be considered to be entitled to access the confidential information. Tokens, or any other suitable proxy for the confidential information, can be generated and associated with the confidential information. These tokens can then be provided to devices in a low-trust network that are not entitled to access the confidential information. Devices in the low-trust network can then generate

documents with the tokens embedded therein (which may be referred to herein as an unenriched document) and devices in the high-trust networks can receive the documents, replace the tokens with appropriate confidential information (to create enriched documents), and present the documents to users using user devices on the high-trust network.

[0025] As described above and further below, these mechanisms provide an important technical solution to the problem of securely generating documents that contain confidential information without risking exposing the confidential information in low-trust networks. The mechanism enables an organization to use a vendor to generate documents that will ultimately contain confidential information without providing the confidential information to the vendor. Because the vendor does not have access to the confidential information, the organization and the vendor do not have to worry about confidential information being stolen or misused from the vendor's computers, and this protects the organization and the vendor from liability and revenue loss that would be associated with such theft and misuse.

[0026] Turning to FIG. 1, an example 100 of a system for generating documents containing confidential information in accordance with some embodiments is shown. As illustrated, system 100 includes a low-trust server 104 in a low-trust network 102, a communication network 106, a high-trust server 110 in a high-trust network 108, one or more user devices 112 in the high-trust network, and communication links 114. Any other suitable components can be included in system 100.

[0027] Low-trust server 104 can be any suitable computing device that is not entitled to access certain confidential information. In some embodiments, low-trust server 104 can provide and/or generate documents to be enriched with the confidential information and/or perform any other suitable functions. While only one low-trust server 104 is shown in FIG. 1, any suitable number of low-trust servers can be used in some embodiments.

[0028] As shown in FIG. 1, low-trust server 104 can be part of a low-trust network 102 having devices that are not entitled to access certain confidential information. For example, low-trust network 102 can be a network maintained by a vendor that is not entitled to access the confidential information of a organization.

[0029] High-trust server 110 can be any suitable computing device that is entitled to access certain confidential information. In some embodiments, high-trust server 110 can enrich documents with confidential information and/or perform any other suitable functions. While only one high-trust server 110 is shown in FIG. 1, any suitable number of high-trust servers can be used in some embodiments.

[0030] User devices 112 can be any suitable devices for accessing certain confidential information as part of enriched documents. An example of a manner in which such enriched documents can be requested and provided is described below in connection with FIG. 8. While two user devices 112 are shown in FIG. 1, any suitable number of user devices can be used in some embodiments.

[0031] In some embodiments, user devices 112 can be any devices suitable for requesting and presenting enriched documents and/or performing any other suitable functions. For example, in some embodiments, user devices 112 can include a mobile device, such as a mobile phone, a tablet computer, a wearable computer, a laptop computer, and/or any other suitable mobile device. As another example, in some embodiments, user devices 112 can include a non-mobile device, such as a television, a projector device, a game console, desktop computer, and/or any other suitable non-mobile device.

[0032] As shown in FIG. 1, high-trust server 110 and user devices 112 can be part of a high-trust network 108 having devices that are entitled to access certain confidential information. For

example, high-trust network 108 can be a network maintained by an organization that is entitled to access the confidential information.

[0033] Communication network 106 can be any suitable combination of one or more wired and/or wireless networks in some embodiments. For example, communication network 106 can include any one or more of the Internet, an intranet, a wide-area network (WAN), a local-area network (LAN), a wireless network, a digital subscriber line (DSL) network, a frame relay network, an asynchronous transfer mode (ATM) network, a virtual private network (VPN), and/or any other suitable communication network.

[0034] Servers 104 and 110 and user devices 112 can be connected by one or more communications links 114 to communication network 106. The communications links can be any communications links suitable for communicating data among servers 104 and 110 and user devices 112, such as network links, dial-up links, wireless links, hard-wired links, any other suitable communications links, or any suitable combination of such links. In some embodiments, connections to communication network 106 can be through any suitable device, such as router, switch, gateway, and/or any other suitable device (not shown).

[0035] Servers 104 and/or 110 and/or user devices 112 can be implemented using any suitable hardware in some embodiments. For example, in some embodiments, Servers 104 and/or 110 and/or user devices 112 can be implemented using any suitable general-purpose computer or special-purpose computer. For example, a mobile phone may be implemented using a special-purpose computer. Any such general-purpose computer or special-purpose computer can include any suitable hardware. For example, as illustrated in example hardware 200 of FIG. 2, such hardware can include hardware processor 202, memory and/or storage 204, an input device controller 206, an input device 208, display/audio drivers 210, display and audio output circuitry 212, communication interface(s) 214, an antenna 216, and a bus 218.

[0036] Hardware processor 202 can include any suitable hardware processor, such as a microprocessor, a micro-controller, digital signal processor(s), dedicated logic, and/or any other suitable circuitry for controlling the functioning of a general-purpose computer or a special-purpose computer in some embodiments. In some embodiments, hardware processor 202 can be controlled by a computer program stored in memory and/or storage 204. For example, in some embodiments, the computer program can cause hardware processor 202 to perform functions described herein.

[0037] Memory and/or storage 204 can be any suitable memory and/or storage for storing programs, data, documents, and/or any other suitable information in some embodiments. For example, memory and/or storage 204 can include random access memory, read-only memory, flash memory, hard disk storage, optical media, and/or any other suitable memory.

[0038] Input device controller 206 can be any suitable circuitry for controlling and receiving input from one or more input devices 208 in some embodiments. For example, input device controller 206 can be circuitry for receiving input from a touchscreen, from a keyboard, from a mouse, from one or more buttons, from a voice recognition circuit, from a microphone, from a camera, from an optical sensor, from an accelerometer, from a temperature sensor, from a near field sensor, and/or any other type of input device.

[0039] Display/audio drivers 210 can be any suitable circuitry for controlling and driving output to one or more display/audio output devices 212 in some embodiments. For example, display/audio drivers 210 can be circuitry for driving a touchscreen, a flat-panel display, a cathode ray tube display, a projector, a speaker or speakers, and/or any other suitable display and/or presentation devices.

[0040] Communication interface(s) 214 can be any suitable circuitry for interfacing with one or more communication networks, such as network 106 as shown in FIG. 1. For example,

interface(s) 214 can include network interface card circuitry, wireless communication circuitry, and/or any other suitable type of communication network circuitry.

[0041] Antenna 216 can be any suitable one or more antennas for wirelessly communicating with a communication network (e.g., communication network 106) in some embodiments. In some embodiments, antenna 216 can be omitted.

[0042] Bus 218 can be any suitable mechanism for communicating between two or more components 202, 204, 206, 210, and 214 in some embodiments.

[0043] Any other suitable components can be included in hardware 200 in accordance with some embodiments.

[0044] Turning to FIGS. 3 and 4, examples 300 and 400 of an unenriched document and an enriched document, respectively, are shown in accordance with some embodiments.

[0045] In FIG. 3, an example unenriched document 300 for a "CAPITAL CALL NOTICE" is shown. It should be understood that document 300 can be for any suitable purpose and can have any suitable content in some embodiments. As also shown, document 300 includes a token 302 that identifies confidential information that can be used to enrich the document. While only one token is included in document 300, any suitable number of tokens and types of tokens can be used in some embodiments. In some embodiments, token 302 can include two pieces of information: (1) an identifier of a record ("93c31348-2535-4b36-927e-25b6ee37ffad"); and (2) an identifier of a field within the record ("account_name"). The identified record and field can be used to place confidential information in the unenriched document. For example, as shown in document 400 of FIG. 4, token 302 has been replaced with confidential information ("John J Smith") 402.

[0046] Turning to FIG. 5, an example 500 of a record for storing an entity's confidential information (in this case, a person's confidential information, though confidential information

can be stored for any suitable type of entity in some embodiments), and an anonymized record 502 for linking to such confidential information is illustrated in accordance with some embodiments.

[0047] As shown, record 500 includes fields for an entity identifier ("93c31348-2535-4b36-927e-25b6ee37ffad"), an account name ("John J Smith"), a first name ("John"), a middle name ("J"), a last name ("Smith"), one or more address identifiers ("a4d42459-3646-5c47-a38f-36c7ff4800be"), one or more phone numbers ("212-555-1212; 646-555-1212"), one or more account identifiers ("aea9d156-e7fe-4494-a94a-86d8c983c25f"), a tax identifier ("999-99-9999"), and a net worth ("1,000,000.00"). Record 500 can be stored on high-trust server 110 in some embodiments.

[0048] While specific fields are provided in FIG. 5 for purposes of illustration, it should be understood that any suitable number and type of fields can be used in some embodiments.

[0049] Entity identifier ("93c31348-2535-4b36-927e-25b6ee37ffad") can be used to uniquely identify the record for "John J Smith" in unenriched documents.

[0050] Address identifier(s) ("a4d42459-3646-5c47-a38f-36c7ff4800be") and account identifier(s) ("aea9d156-e7fe-4494-a94a-86d8c983c25f") can be used to identify address record(s) and account record(s) associated with "John J Smith".

[0051] Once record 500 is anonymized, the record can appear as shown by anonymized record 502. Record 502 can be stored on low-trust server 104 in some embodiments.

[0052] As shown, record 502 can replace the account name with "93c31348-2535-4b36-927e-25b6ee37ffad\$\$account_name", the first name with "93c31348-2535-4b36-927e-25b6ee37ffad\$\$first_name", the middle name with "93c31348-2535-4b36-927e-25b6ee37ffad\$\$middle_name", the last name with "93c31348-2535-4b36-927e-25b6ee37ffad\$\$last_name", the phone number(s) with "93c31348-2535-4b36-927e-

25b6ee37ffad\$\$phone", the tax identifier with "93c31348-2535-4b36-927e-25b6ee37ffad\$\$tax_id", and the net worth with "93c31348-2535-4b36-927e-25b6ee37ffad\$\$net_worth".

[0053] Turning to FIG. 6, an example 600 of a record for storing an entity's address confidential information, and an anonymized record 602 for linking to such confidential information is illustrated in accordance with some embodiments.

[0054] As shown, record 600 includes fields for an address identifier ("a4d42459-3646-5c47-a38f-36c7ff4800be"), an address line 1 ("123 Main Street"), an address line 2 ("Apt 1A"), a city ("New York"), a state ("New York"), a postal code ("10001"), and a country ("US"). Record 600 can be stored on high-trust server 110 in some embodiments.

[0055] While specific fields are provided in FIG. 6 for purposes of illustration, it should be understood that any suitable number and type of fields can be used in some embodiments.

[0056] Address identifier ("a4d42459-3646-5c47-a38f-36c7ff4800be") can be used to uniquely identify the record for the address in unenriched documents.

[0057] Once record 600 is anonymized, the record can appear as shown by anonymized record 602. Record 602 can be stored on low-trust server 104 in some embodiments.

[0058] As shown, record 602 can replace the address line 1 with "a4d42459-3646-5c47-a38f-36c7ff4800be\$\$addr1", the address line 2 with "a4d42459-3646-5c47-a38f-36c7ff4800be\$\$addr2", the city with "a4d42459-3646-5c47-a38f-36c7ff4800be\$\$city", the state with "a4d42459-3646-5c47-a38f-36c7ff4800be\$\$state", the postal code with "a4d42459-3646-5c47-a38f-36c7ff4800be\$\$postal", and the country with "a4d42459-3646-5c47-a38f-36c7ff4800be\$\$country".

[0059] Turning to FIG. 7, an example 700 of a record for storing an entity's account confidential information, and an anonymized record 702 for linking to such confidential information is illustrated in accordance with some embodiments.

[0060] As shown, record 700 includes fields for an account identifier ("aea9d156-e7fe-4494-a94a-86d8c983c25f"), an account name ("John J Smith"), an account number ("123456789"), entity identifier(s) ("93c31348-2535-4b36-927e-25b6ee37ffad"), address identifier(s) ("a4d42459-3646-5c47-a38f-36c7ff4800be"), and a balance ("50,000.00"). Record 700 can be stored on high-trust server 110 in some embodiments.

[0061] While specific fields are provided in FIG. 7 for purposes of illustration, it should be understood that any suitable number and type of fields can be used in some embodiments.

[0062] Entity identifier(s) ("93c31348-2535-4b36-927e-25b6ee37ffad") can be used to uniquely identify the entity (entities) for the account in unenriched documents. Address identifier(s) ("a4d42459-3646-5c47-a38f-36c7ff4800be") can be used to uniquely identify the address(es) for the account in unenriched documents.

[0063] Once record 700 is anonymized, the record can appear as shown by anonymized record 702. Record 702 can be stored on low-trust server 104 in some embodiments.

[0064] As shown, record 702 can replace the account name with "aea9d156-e7fe-4494-a94a-86d8c983c25f\$\$account_name", the account number with "aea9d156-e7fe-4494-a94a-86d8c983c25f\$\$acct_no", and the country with "aea9d156-e7fe-4494-a94a-86d8c983c25f\$\$balance".

[0065] Turning to FIG. 8, an example 800 of a process for providing an enriched document to a user of a user device in accordance with some embodiments is shown. As illustrated, process 800 can be implemented as three subprocesses 802, 804, and 806 that are executed on

low-trust server 104, high-trust server 110, and a user device 112, respectively, in some embodiments.

[0066] Process 800 can begin in some embodiments by making a request for a document with confidential information at 808. This request can be made in any suitable manner in some embodiments. For example, in some embodiments, a user of a user device 112 can click on a link in a web browser for a document, and the browser can send a suitable request to low-trust server 104. As another example, in some embodiments, a user of a user device 112 can click on a menu option in an app, and the app can send a suitable request to low-trust server 104. The request can then be received at 810.

[0067] Next, at 812, process 800 can generate the requested document with one or more tokens filling any fields in the document that will contain confidential information. The document can have any suitable content, and any suitable number and type of tokens can be present in the document. As described above, an example of a document with a token is shown in FIG. 3.

[0068] The generated document can then be transmitted from low-trust server 104 to high-trust server 110 at 814. The high-trust server can receive the document at 816.

[0069] At 818, the high-trust server can replace the tokens with confidential information to produce an enriched document. For example, the high-trust server can scan the document for tokens and for each token found, the server can search a database for the confidential information corresponding to that token and replace the token in the document with the confidential information.

[0070] Next, at 820, process 800 can store the enriched document in a server. In some embodiments, this server can be the high-trust server or any other suitable server. In some embodiments, this server can be located on high-trust network 108.

[0071] A uniform resource locator (URL) corresponding to the enriched document can then be transmitted to low-trust server 104 at 822. The low-trust server can receive the URL at 824.

[0072] Then, at 826, the low-trust server can transmit the URL to user device 112 in response to the request made at 808. The URL can be received by the user device at 828.

[0073] Next, at 830, the user device can request the enriched document from the server on which the document was stored at 820 using the URL.

[0074] At 832, the server on which the document was stored at 820 can serve the document to the user device. In some embodiments, this server will only serve the document to the user device when the user device is in high-trust network 108. That is, if the user device is outside high-trust network 108, this server may skip providing the document to the user device in some embodiments.

[0075] Finally, at 834, the user device can receive the enriched document and present it in any suitable manner (such as by displaying it on a screen on the user device, causing it to be printed by a printer coupled to the user device, etc.).

[0076] Turning to FIG. 9, an example 900 of a process for synchronizing confidential information and tokens is shown in accordance with some embodiments. As shown process 900 can be implemented as two subprocesses 902 and 904 that are executed on high-trust server 110 and low-trust server 104, respectively, in some embodiments.

[0077] Process 900 can begin by receiving confidential information 906 at 908. Any suitable confidential information can be received, and this confidential information can be received in any suitable manner from any suitable source. For example, confidential information such as entity information, address information, and account information as described in connection with FIGS. 5-7 can be received in some embodiments. As another example, in some embodiments, this confidential information can be received as an upload from a comma-separated-value (CSV)

file, as a hyper-text transfer protocol (http) post message, as a web hook, and/or in any other suitable manner.

[0078] Next, at 910, process 900 can generate anonymized information. This anonymized information can be generated in any suitable manner. For example, an identifier of a record for the confidential information can be generated as a hash (e.g., MD5) of a portion of the confidential information. As another example, an identifier of a record for the confidential information can be randomly or pseudo-randomly generated and confirmed as not being duplicative of an already-generated identifier. The generated identifier and field names can then be used to anonymize the confidential information as described above in connection with FIGS. 5-7.

[0079] Then, at 912, process 900 can transmit the anonymized information to low-trust server 104. This anonymized information can then be received by the low-trust server at 914.

[0080] Finally, at 916, the low-trust server can store the anonymized information in any suitable manner.

[0081] It should be understood that at least some of the above-described blocks of the processes of FIGS. 8 and 9 can be executed or performed in any order or sequence not limited to the order and sequence shown in and described in connection with the figures. Also, some of the above blocks of the processes of FIGS. 8 and 9 can be executed or performed substantially simultaneously where appropriate or in parallel to reduce latency and processing times. Additionally or alternatively, some of the above described blocks of the processes of FIGS. 8 and 9 can be omitted.

[0082] In some implementations, any suitable computer readable media can be used for storing instructions for performing the functions and/or processes described herein. For example, in some implementations, computer readable media can be transitory or non-

transitory. For example, non-transitory computer readable media can include media such as non-transitory forms of magnetic media (such as hard disks, floppy disks, etc.), non-transitory forms of optical media (such as compact discs, digital video discs, Blu-ray discs, etc.), non-transitory forms of semiconductor media (such as flash memory, electrically programmable read only memory (EPROM), electrically erasable programmable read only memory (EEPROM), etc.), any suitable media that is not fleeting or devoid of any semblance of permanence during transmission, and/or any suitable tangible media. As another example, transitory computer readable media can include signals on networks, in wires, conductors, optical fibers, circuits, any suitable media that is fleeting and devoid of any semblance of permanence during transmission, and/or any suitable intangible media.

[0083] Although the invention has been described and illustrated in the foregoing illustrative embodiments, it is understood that the present disclosure has been made only by way of example, and that numerous changes in the details of implementation of the invention can be made without departing from the spirit and scope of the invention, which is limited only by the claims that follow. Features of the disclosed embodiments can be combined and rearranged in various ways.

What is claimed is:

1. A system for generating documents with confidential information, comprising:
a memory; and
a first collection of at least of one hardware processor coupled to the memory and configured to:
receive from a user device a request for a first document with confidential information;
generate a second document, that corresponds to the first document, with at least one token corresponding to the confidential information;
transmit the second document to a second collection of at least one hardware processor in a high-trust network that is entitled to access the confidential information;
receive from the second collection of at least one hardware processor in the high-trust network a uniform resource locator (URL) corresponding to the first document; and
transmit the URL to the user device.
2. The system of claim 1, wherein the user device is in the high trust network.
3. The system of claim 1, wherein the second collection of at least one hardware processor in the high-trust network is in a server.
4. The system of claim 3, wherein the first document is stored on the server.
5. The system of claim 1, wherein the second collection of at least one hardware processor configured to:

receive the second document from the first collection of at least one hardware processor;

replace the at least one token in the second document to produce the first document;

cause the first document to be stored; and

transmit the URL to the first collection of at least one hardware processor.

6. The system of claim 5, wherein the second collection of at least one hardware processor is further configured to serve the first document to the user device.

7. The system of claim 1, wherein the user device is configured to:

send the request for the first document to the first collection of at least one hardware processor;

receive the URL;

request the first document using the URL;

receive the first document; and

cause the first document to be presented.

8. A system for generating documents with confidential information, comprising:

a memory; and

a first collection of at least of one hardware processor coupled to the memory and configured to:

receive a first document from a second collection of at least one hardware processor;

replace at least one token in the first document to produce a second document;
cause the second document to be stored; and
transmit a uniform resource locator (URL) corresponding to the second document
to the second collection of at least one hardware processor.

9. The system of claim 8, wherein the first collection of at least one hardware processor
is further configured to serve the first document to a user device.

10. The system of claim 9, wherein the user device is configured to:
send a request for the first document to the first collection of at least one hardware
processor;
receive the URL;
request the first document using the URL;
receive the first document; and
cause the first document to be presented.

11. The system of claim 8, wherein the second collection of at least one hardware
processor is configured to:
generate the first document, that corresponds to the second document, with at
least one token corresponding to confidential information;
transmit the first document to the first collection of at least one hardware
processor in a high-trust network that is entitled to access the confidential information;
receive from the first collection of at least one hardware processor in the high-
trust network a uniform resource locator (URL) corresponding to the second document; and

transmit the URL to a user device.

12. The system of claim 11, wherein the user device is in a high trust network.
13. The system of claim 8, wherein the first collection of at least one hardware processor is in a server.
14. The system of claim 13, wherein the second document is stored on the server.
15. A system for generating documents with confidential information, comprising:
a user device configured to:
 send a request for a first document with confidential information to a first collection of at least one hardware processor in a low-trust network that is not entitled to access the confidential information;
 receive a uniform resource locator (URL) corresponding to the first document from the first collection of at least one hardware processor;
 request the first document using the URL from a second collection of at least one hardware processor in a high-trust network that is entitled to access the confidential information;
 receive the first document; and
 cause the first document to be presented.
16. The system of claim 15, wherein the user device is in the high trust network.

17. The system of claim 15, wherein the second collection of at least one hardware processor in the high-trust network is in a server.
18. The system of claim 17, wherein the first document is stored on the server.
19. The system of claim 18, wherein the first collection of at least of one hardware processor is configured to:
- receive from the user device the request for the first document;
 - generate a second document, that corresponds to the first document, with at least one token corresponding to the confidential information;
 - transmit the second document to the second collection of at least one hardware processor;
 - receive from the second collection of at least one hardware processor a uniform resource locator (URL) corresponding to the first document; and
 - transmit the URL to the user device.
20. The system of claim 19, wherein the second collection of at least one hardware processor is configured to:
- receive the second document from the first collection of at least one hardware processor;
 - replace the at least one token in the second document to produce the first document;
 - cause the first document to be stored; and
 - transmit the URL to the first collection of at least one hardware processor.

21. The system of claim 20, wherein the second collection of at least one hardware processor is further configured to serve the first document to the user device.