

SELF-SERVICE AUTHENTICATED PRINTING

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to U.S. Patent Application Serial No. 18/195,550, filed May 10, 2023, the disclosure of which is incorporated herein by reference in its entirety.

BACKGROUND

[0002] The present application relates to computing technology and facilitates a self-service printing using authentication for improved data security.

[0003] Often times physical copies of digital documents and other material are required and/or preferred for consumption of information in such documents and material. However, not everyone may have access to a private printer. Although public printers, such as at libraries, retail stores, may be available, sensitive information, such as confidential, or privileged information, may prohibit the use of such printers. Moreover, the documents may require special printing, such as in the case of certain financial documents (e.g., checks), certain legal documents (e.g., stamp paper), etc. Printing such documents may require access to specialized printers. Accordingly, there is a need to print documents and other material in an authenticated and secure manner to prevent the printed copies from being accessed by third parties.

SUMMARY

[0004] According to one or more aspects, a computer-implemented method to enable self-service printing with authentication includes receiving, by a server, a print-request to print a document associated with an account, the print-request received from a computing device. The method further includes adding, by the server, a print job for the document in a print queue associated with the account. The method further includes receiving, by the server, a second request to initiate printing the document associated with the account, the second request received from a printer. The method further includes releasing, by the server, the print queue associated with the account to cause the printer to print the document, the releasing being responsive to the second request being authenticated.

[0005] According to one or more aspects, a computer-implemented method to enable self-service printing with authentication includes selecting, by a computing device, for printing, a document associated with an account. The method further includes generating, by the computing device, a list of printers for printing the document, the list is generated based on a

type of the document. The method further includes selecting, by the computing device, from the list, a printer to print the document. The method further includes providing, by the computing device, in response to the printer being accessed to print the document, an authentication code that causes the printer to print the document.

[0006] According to one or more aspects, a computing apparatus includes a processor, and a memory storing instructions that, when executed by the processor, configure the computing apparatus to receive a first request to print a document associated with an account, the first request received from a computing device. The computing apparatus is further configured to add a print job for the document in a print queue associated with the account. The computing apparatus is further configured to receive a second request to initiate printing the document associated with the document, the second request received from a printer. The computing apparatus is further configured to release the print queue associated with the account to cause the printer to print the document, the release being responsive to the second request being authenticated.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

[0007] To easily identify the discussion of any particular element or act, the most significant digit or digits in a reference number refer to the figure number in which that element is first introduced.

[0008] FIG. 1 illustrates an aspect of the subject matter in accordance with one embodiment.

[0009] FIG. 2A illustrates an aspect of the subject matter in accordance with one embodiment.

[0010] FIG. 2B illustrates an aspect of the subject matter in accordance with one embodiment.

[0011] FIG. 3 illustrates an aspect of the subject matter in accordance with one embodiment.

[0012] FIG. 4 illustrates a routine 400 in accordance with one embodiment.

[0013] FIG. 5 illustrates a routine 500 in accordance with one embodiment.

[0014] FIG. 6 illustrates a routine 600 in accordance with one embodiment.

[0015] FIG. 7A illustrates a contactless card in accordance with one embodiment.

[0016] FIG. 7B illustrates a contactless card 102 in accordance with one embodiment.

[0017] FIG. 8 illustrates a data structure 800 in accordance with one embodiment.

[0018] FIG. 9 illustrates a computer architecture 900 in accordance with one embodiment.

[0019] FIG. 10 illustrates a sequence flow 1000 in accordance with one embodiment.

[0020] FIG. 11 is a diagram of a key system according to an example embodiment.

[0021] FIG. 12 is a flowchart of a method of generating a cryptogram according to an example embodiment.

[0022] FIG. 13 illustrates an aspect of the subject matter in accordance with one embodiment.

DETAILED DESCRIPTION

[0023] Embodiments disclosed herein provide techniques for secure printing of material using a contactless card to authenticate the user and to verify his/her presence at the time of printing and/or releasing the printed material. To create a print request via a computing device, the computing device may authenticate the user using a contactless card, e.g., using a cryptogram generated by the contactless card. An application executing on the computing device may receive the cryptogram via communications with the contactless card and transmit the cryptogram to a server for verification. The server may give the user access to request printing one or more printable material (e.g., documents, images, etc.) based on verification of the cryptogram. The printable material may be previously generated or dynamically generated upon user's request.

[0024] The server may add the requested material to a printing queue. The print queue may be maintained by the server. In some examples, the user may designate a printer. The printer may be a printer device identified as a secure trusted printer by the server. The designated printer may maintain the print queue in some examples. In some examples, the print queue may be specific to the user, the contactless card, or an account associated with the user. Once the user claims to be at a secure trusted printer or at the designated printer, he/she can cause the material to be printed and/or released by authenticating and verifying his/her presence using a contactless card. The same contactless card used at the time of requesting the printing may be required to release the printable material in some cases. Alternatively, different contactless cards associated with the user, or the account, may be used at the time of requesting and releasing.

[0025] The server may securely transmit the printable material to the printer. In some embodiments, when the user attempts to release the printable material to generate printed copies, cryptographic verification using the contactless card may be used to authenticate access to the printable material in a print queue. For example, the user may provide the contactless card to the printer, and the printer or associated card reader may read the card and receive the

cryptogram. The printer may provide the cryptogram to a server to perform authentication of the user. If the cryptographic verification is not successful, the user may be restricted from accessing the printable material, thereby improving the security of the account.

[0026] As additional or alternative security, the user may have to perform a multi-factor authentication to release the printable material from the print queue at the printer. The multi-factor authentication may include using a combination of the contactless card, the computing device, and one or more authentication credentials of the user associated with the account.

[0027] Embodiments disclosed herein provide secure techniques to print one or more documents using cryptograms generated by contactless cards and other security measures. By leveraging cryptograms, embodiments of the disclosure may securely verify the identity and presence of the user with minimal risk of fraudulent activity associated with the printed copies. Furthermore, embodiments disclosed herein facilitate a user to print material in a secure manner when the user may not have access to a printer. Further still, embodiments disclosed herein facilitate a server and/or a printer to limit printing of material only to verified users and/or only when the authenticated user is physically present at the printer.

[0028] With general reference to notations and nomenclature used herein, the detailed descriptions herein may be presented in terms of program procedures executed on a computer or network of computers. These procedural descriptions and representations are used by those skilled in the art to effectively convey the substance of their work to others skilled in the art.

[0029] A procedure is here, and generally, conceived to be a self-consistent sequence of operations leading to a desired result. These operations are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical, magnetic, or optical signals capable of being stored, transferred, combined, compared, and otherwise manipulated. It proves convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like. It should be noted, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to those quantities.

[0030] Further, the manipulations performed are often referred to in terms, such as adding or comparing, which are commonly associated with mental operations performed by a human operator. No such capability of a human operator is necessary, or desirable in most cases, in any of the operations described herein, which form part of one or more embodiments. Rather,

the operations are machine operations. Useful machines for performing operations of various embodiments include digital computers or similar devices.

[0031] Some embodiments may be described using the expression "coupled" and "connected" along with their derivatives. These terms are not necessarily intended as synonyms for each other. For example, some embodiments may be described using the terms "connected" and/or "coupled" to indicate that two or more elements are in direct physical or electrical contact with each other. The term "coupled," however, may also mean that two or more elements are not in direct contact with each other, but yet still co-operate or interact with each other.

[0032] Various embodiments also relate to apparatus or systems for performing these operations. This apparatus may be specially constructed for the required purpose, or it may comprise a computer as selectively activated or reconfigured by a computer program stored in the computer. The procedures presented herein are not inherently related to a particular computer or other apparatus. Various machines may be used with programs written in accordance with the teachings herein, or it may prove convenient to construct more specialized apparatus to perform the required method steps. The required structure for a variety of these machines will appear from the description given.

[0033] Reference is now made to the drawings, wherein like reference numerals are used to refer to like elements throughout. In the following description, for purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding thereof. However, the novel embodiments can be practiced without these specific details. In other instances, structures and devices are shown in block diagram form in order to facilitate a description thereof. The intention is to cover all modifications, equivalents, and alternatives consistent with the claimed subject matter.

[0034] In the Figures and the accompanying description, the designations "a" and "b" and "c" (and similar designators) are intended to be variables representing any positive integer. Thus, for example, if an implementation sets a value for $a = 5$, then a complete set of components 123 illustrated as components 123-1 through 123- a (or 123a) may include components 123-1, 123-2, 123-3, 123-4, and 123-5. The embodiments are not limited in this context.

[0035] Embodiments disclosed herein provide techniques to address one or more technical challenges. The technical challenges are related to securely printing material, such as documents, images, etc., from a user's account. The technical challenges addressed herein includes to be able to securely print material from a user's account when the user does not have

access to a private printer. Embodiments herein address such a technical challenge by using a contactless card to authenticate and verify the user at the time of printing. Additional security can be provided in some embodiments by using a combination of the contactless card and a computing device (e.g., mobile). Accordingly, technical solutions and improvements are provided to increase security of data access.

[0036] Embodiments herein are solutions to internet-centric challenges where data stored in servers (e.g., cloud platform) has to be securely accessed and printed using a public printer. By using one or more of the contactless cards and a computing device, the secure access and printing is facilitated.

[0037] Additional improvements and applications provided by embodiments herein include location-based enhancements to identify printers within a predetermined range from the user, such that the identified printer is capable of printing material requested by the user. Further, improvements provided by embodiments described herein also include dynamically generating and printing material based on the user's request when the authorized user is verified to be present at the printer.

[0038] Several other improvements to technology, such as printers and servers, to facilitate secure printing and advantages in such technical areas will be apparent to a person skilled in the art based on the description herein.

[0039] With general reference to notations and nomenclature used herein, one or more portions of the detailed description which follows may be presented in terms of program procedures executed on a computer or network of computers. These procedural descriptions and representations are used by those skilled in the art to convey the substances of their work most effectively to others skilled in the art. A procedure is here, and generally, conceived to be a self-consistent sequence of operations leading to a desired result. These operations are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical, magnetic, or optical signals capable of being stored, transferred, combined, compared, and otherwise manipulated. It proves convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like. It should be noted, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to those quantities.

[0040] Further, these manipulations are often referred to in terms, such as adding or comparing, which are commonly associated with mental operations performed by a human operator. However, no such capability of a human operator is necessary, or desirable in most cases, in any of the operations described herein that form part of one or more embodiments. Rather, these operations are machine operations. Useful machines for performing operations of various embodiments include digital computers as selectively activated or configured by a computer program stored within that is written in accordance with the teachings herein, and/or include apparatus specially constructed for the required purpose or a digital computer. Various embodiments also relate to apparatus or systems for performing these operations. These apparatuses may be specially constructed for the required purpose. The required structure for a variety of these machines will be apparent from the description given.

[0041] Reference is now made to the drawings, wherein like reference numerals are used to refer to like elements throughout. In the following description, for the purpose of explanation, numerous specific details are set forth in order to provide a thorough understanding thereof. It may be evident, however, that the novel embodiments can be practiced without these specific details. In other instances, well-known structures and devices are shown in block diagram form in order to facilitate a description thereof. The intention is to cover all modification, equivalents, and alternatives within the scope of the claims.

[0042] FIG. 1 depicts an exemplary system 100, also referred to as a computing architecture, consistent with disclosed embodiments. Although the system 100 shown in Figures herein has a limited number of elements in a certain topology, it may be appreciated that the system 100 may include more or less elements in alternate topologies as desired for a given implementation.

[0043] The system 100 comprises one or more contactless cards 102, one or more computing devices 104, one or more servers 106, and one or more printers 108.

[0044] The contactless card 102 is representative of any type of card, such as a credit card, debit card, automated teller machine (ATM) card, gift card, payment card, smart card, identification card, and the like. The contactless card 102 is associated with an account 142 of a user 110. The account 142 can be a financial account, a social media account, an employee account, a customer loyalty account (e.g., airline, hotel, restaurant, store, etc.), or any other account associated with the user 110. The user 110 may perform one or more operations using the account 142, and or associated with the account 142. For example, in case of a financial

account, the user 110 may conduct transactions such as money transfers, check deposits, bill payments, balance inquiries, reaching customer service, accessing one or more documents, etc. In case of an employee account, the user 110 may conduct operations such as sending/receiving messages, editing documents/records, operating machinery, etc., or any other operations that the user 110 may be expected to perform as part of his/her employment. Messages can be emails, instant messages, or any other types of messages. In case of a loyalty account, the user 110 may perform operations such as purchases, returns, statement inquiries, receipt inquiries, accessing coupons, etc. It is understood that the account 142 can be any type of account, and not limited to the types of accounts listed herein.

[0045] The contactless card 102 facilitates authenticating the user 110 to use the account 142. Here, “using” the account 142 can include any operation performed associated with the account 142. For example, using the account can include performing one or more operations associated with the account 142, such as logging into the account 142, accessing resources associated with the account 142, etc. In addition, using the account 142 can include accessing and/or changing one or more settings of the account 142. For example, the settings can include usernames, passwords, demographic information (age, address, gender, etc.), biometric identifiers, financial information (e.g., debt limit, transaction limits, etc.), notification settings (e.g., condition when to generate and send notifications to user 110), etc. The settings can also include access permissions that provide/limit the user's 110 access to one or more physical/digital resources associated with the account 142. The physical resources can include doors, safes, computers, cabinets, devices (e.g., printers, projectors, etc.), apparatus (e.g., lab apparatus, etc.), or any other such resources. Digital resources can include files, computers, other user accounts, databases, etc. Based on the access permissions of the user 110 specified by the account 142, he/she may or may not be authorized to access one or more of the resources (physical/digital). The contactless card 102 addresses the challenge of authenticating the user 110 as described herein.

[0046] The account 142 is maintained by the account provider (not shown). The account provider of the account 142 can be a financial institution (e.g., bank, credit union, etc.), an employer, a social media platform, an airline, a restaurant, a hotel, a retailer, or any other entity. The account provider provides the account 142 using a server 106.

[0047] As shown, the server 106 includes an authentication application 138 and an account database 128. The account database 128 generally includes information related to one or more

accounts, (e.g., account 142), one or more users (e.g., user 110), and one or more contactless cards 102 of the account 142. The account 142 includes the permissions, settings, and other information that facilitates the user 110 to use the account 142 with the contactless card 102. Further, the user 110 can use the account 142 via the computing device 104. In some embodiments, the user 110 can use the account 142 via a combination of the contactless card 102 and the computing device 104. For example, the combination of the contactless card 102 and the computing device 104 is used to perform a multi-factor authentication (MFA) of the user 110. Embodiments described herein, accordingly address a technical challenge of authenticating access to the account 142, which is an electronic account. Embodiments herein, accordingly, address an internet-centric, digital-account-centric challenges in a practical manner. The challenges are addressed using specific computer components, that facilitate authenticating the user 110 by performing a specific sequence of operations.

[0048] The computing device 104 is representative of any number and type of computing devices, such as smartphones, tablet computers, wearable devices, laptops, portable gaming devices, virtualized computing system, merchant terminals, point-of-sale systems, servers, desktop computers, and the like. A mobile device may be used as an example of the computing device 104 but should not be considered limiting of the disclosure. The server 106 is representative of any type of computing device, such as an enterprise server, workstation, compute cluster, cloud computing platform, virtualized computing system, and the like. Although not depicted for the sake of clarity, the computing device 104, contactless card 102, and server 106 each include one or more memory devices (e.g., random access memory, storage drives, etc.), one or more processor circuits (central processing unit, graphics processing unit, floating point unit, etc.), to execute programs, code, scripts, and other types of computer-executable instructions.

[0049] The contactless card 102 includes one or more communications interfaces 126, such as a radio frequency identification (RFID) chip configured to communicate with a communications interface 126 (also referred to herein as a “card reader”, a “wireless card reader”, and/or a “wireless communications interface”) of the computing devices 104. The communications interfaces 126 may facilitate wireless communication via near field communication (NFC), using the Europay, Mastercard, and VISA standard (EMV), or other short-range protocols in wireless communication. Although NFC is used as an example

communications protocol herein, the disclosure is equally applicable to other types of wireless communications, such as Bluetooth™, Bluetooth Low Energy (BLE), and/or Wi-Fi™, etc.

[0050] As shown, a memory 112 of the contactless card 102 includes a unique ID 114, an applet 116, one or more master keys 118, a counter 120, and one or more diversified keys 122. The unique ID 114 may be any identifier that uniquely identifies the contactless card 102 relative to other contactless cards 102. In some examples, the unique ID 114 may be an identifier that uniquely identifies user 110 with whom the contactless card 102 is associated. The applet 116 is executable code (i.e., computer-executable instructions) configured to perform some or all of the operations described herein. The counter 120 is a value that is synchronized between the contactless card 102 and server 106. The counter 120 may comprise a number that changes each time data is exchanged between the contactless card 102 and the server 106 (and/or the contactless card 102 and the computing device 104). The counter 120, master keys 118, diversified keys 122, and/or unique ID 114 are used to provide security in the system 100 as described in greater detail below. The memory 112 can include additional components, such as an operating system, images, etc., which are not depicted herein for brevity.

[0051] As shown, a memory 132 of the computing device 104 includes an instance of an operating system 134. Example operating systems include the Android® OS, iOS®, macOS®, Linux®, and Windows® operating systems. As shown, the operating system 134 includes an account application 136. The account application 136 allows the user 110 to perform various account-related operations, such as viewing account balances, purchasing items, processing payments, accessing one or more resources, printing documents, and the like. The account application 136 is a computer program including one or more computer-executable instructions. In some embodiments, the account application 136 can include computer-executable instructions that are specific to the operating system 134 and/or the computing device 104. Alternatively, or in addition, the account application 136 includes computer-executable instructions that can be executed across different operating systems and computing devices. In some embodiments, the account application 136 may be a web browser that allows the user 110 to access the account 142 via one or more web pages of the account 142. The web pages of the account 142 may be hosted by the server 106 (or another hosting entity).

[0052] In some embodiments, the user 110 accesses the account 142 on the server 106 via the account application 136 on the computing device 104 after authenticating using authentication

credentials. For example, the authentication credentials may include a username (or login) and password, biometric credentials (e.g., fingerprints, Face ID, palmprints, iris scans, etc.), and the like. In some embodiments, such authentication credentials-based access only facilitates the user 110 to access a subset of features/resources of the account 142. For example, in case of a financial account, the account application 136 may limit the user 110 to only view certain balances and/or information, but not permit the user to perform operations, such as a money transfer. In case of a loyalty account, the user 110 may be prohibited from purchases at such a first level of authentication that provides access to the subset of features/resources. In case of an employee account, the user 110 may be prohibited from viewing emails, or accessing certain premises, etc. To access such prohibited (or secured, second level) features of the account 142 the user 110 has to be authenticated using the contactless card 102.

[0053] In some embodiments, the user 110 is authenticated using a gesture-based authentication using the contactless card 102. For example, the user 110 may tap the contactless card 102 to the computing device 104 (or otherwise bring the contactless card 102 within communications range of the communications interface 126 of the computing device 104 104). The account application 136 may then instruct the applet 116 to generate a cryptogram 124. The cryptogram 124 may be generated based on any suitable cryptographic technique. In some embodiments, the cryptogram 124 may be based on the unique ID 114 of the contactless card 102. The contactless card 102 transmits the cryptogram 124 to the account application 136 via the communications interfaces 126. In some cases, a wireless communication using NFC is performed by the communications interfaces 126. In some embodiments, the applet 116 may include the cryptogram 124 and an unencrypted identifier (e.g., the counter 120, the unique ID 114, and/or any other unique identifier) as part of a transmitted data package including the cryptogram 124. In at least one embodiment, the data package is an NDEF file.

[0054] In some embodiments, the system 100 is configured to implement key diversification to secure the communicated data, which may be referred to as a key diversification technique herein. Generally, the server 106 and the contactless card 102 may be provisioned with the same master key 118 (also referred to as a master symmetric key). More specifically, each contactless card 102 is programmed with a distinct master key 118 that has a corresponding pair in the server 106. For example, when a contactless card 102 is manufactured, a unique master key 118 may be programmed into the memory 112 of the contactless card 102.

Similarly, the unique master key 118 may be stored in a record of the user 110 associated with the contactless card 102 in the account database 128 of the server 106 (and/or stored in a different secure location, such as the hardware security module (HSM) 130). The master key 118 may be kept secret from all parties other than the contactless card 102 and server 106, thereby enhancing security of the system 100. In some embodiments, the applet 116 of the contactless card 102 may encrypt and/or decrypt data (e.g., the unique ID 114) using the master key 118 and the data as input a cryptographic algorithm. For example, encrypting the unique ID 114 with the master key 118 may result in the cryptogram 124. Similarly, the server 106 may encrypt and/or decrypt data associated with the contactless card 102 using the corresponding master key 118. Because the server 106 and the contactless card 102 have the same master key 118, by using the same cryptographic algorithm, the two generate matching cryptograms 124.

[0055] Accordingly, the user 110 can be authenticated by matching the cryptograms 124 generated by the contactless card 102 and the server 106. In some embodiments, the computing device 104 transmits the cryptogram 124 received from the contactless card 102 to the server 106. The server 106 verifies authentication of the users 110 by comparing the received cryptogram 124 with the cryptogram 124 generated by the server 106. The server 106 sends a notification indicative of the success of the verification to the computing device 104. If the cryptograms 124 match, the server 106 indicates that the verification was successful. Otherwise, the server 106 indicates that the verification was unsuccessful. The server 106 can communicate the notification to the computing device 104 via the network 140, for example.

[0056] In some embodiments, the verification may use additional information apart from the cryptogram 124. Alternatively, or in addition, the cryptogram 124 is generated using data in addition to the unique ID 114. In some embodiments, the master keys 118 of the contactless card 102 and server 106 may be used in conjunction with the counters 120 to enhance security using key diversification. The counters 120 comprise values that are synchronized between the contactless card 102 and server 106. For example, the counters 120 may comprise a number that changes each time data is exchanged between the contactless card 102 and the server 106 (and/or the contactless card 102 and the computing device 104). Here, data exchanged between the contactless card 102 and the server 106 and/or the computing device 104 can include instructions and responses passed between the contactless card 102 and the other device. For example, the applet 116 may provide the master key 118, unique ID 114, and a diversification factor as input to a cryptographic algorithm, thereby producing a diversified key 122. In some

embodiments, the diversification factor is the counter 120. The diversified key 122 may then be used to encrypt some data, such as the diversification factor (e.g., the counter 120) or other sensitive data. The applet 116 and the server 106 may be configured to encrypt the same data to facilitate the decryption and/or verification processing of the cryptogram 124.

[0057] In some embodiments, when preparing to send data (e.g., to the server 106 and/or the computing device 104), the applet 116 of the contactless card 102 may increment the counter 120. The applet 116 of the contactless card 102 may then provide the master keys 118, unique ID 114, and counter 120 as input to a cryptographic algorithm, which produces a diversified key 122 as output. The cryptographic algorithm may include encryption algorithms, hash-based message authentication code (HMAC) algorithms, cipher-based message authentication code (CMAC) algorithms, and the like. Non-limiting examples of the cryptographic algorithm may include a symmetric encryption algorithm such as 3DES or AES107; a symmetric HMAC algorithm, such as HMAC-SHA-256; and a symmetric CMAC algorithm such as AES-CMAC. Examples of key diversification techniques are described in greater detail in United States Patent Application 16/205,119, filed November 29, 2018. The aforementioned patent application is incorporated by reference herein in its entirety.

[0058] The applet 116 may then encrypt some data (e.g., the unique ID 114, the counter 120, a command, and/or any other data) using the diversified key 122 as input to the cryptographic algorithm. For example, encrypting the unique ID 114 the diversified key 122 may result in an encrypted unique ID 114 (e.g., a cryptogram 124).

[0059] In some embodiments, two diversified keys 122 may be generated, e.g., based on one or more portions of the input to the cryptographic function. In some embodiments, the two diversified keys 122 are generated based on two distinct master keys 118, the unique ID 114, and the counter 120. In such embodiments, a message authentication code (MAC) is generated using one of the diversified keys 122, and the MAC may be encrypted using the other one of the diversified keys 122. The MAC may be generated based on any suitable data input to a MAC algorithm, such as sensitive data, the unique ID 114, the counter 120, etc. The applet 116 and the server 106 may be configured to generate the MAC based on the same data. In some embodiments, the cryptogram 124 is included in a data package such as an NDEF file. The account application 1310 may then read the data package including cryptogram 124 via the communications interface 126 of the computing device 104.

[0060] The account application 136 transmits the cryptogram 124 to the server 106. The server 106 may provide the cryptogram 124 to the authentication application 138 and/or the HSM 130 for verification based at least in part on the instance of the master key 118 stored by the server 106. In some embodiments, the authentication application 138 and/or the HSM 130 may identify the master key 118 and counter 120 using the unencrypted unique ID 114 provided to the server 106. In examples where additional data is used to generate the cryptogram 124, the server 106 may identify the additional data in the account database 128 and/or HSM 130 using the unencrypted unique ID 114. In some examples, the authentication application 138 may provide the master key 118, unique ID 114, and counter 120 as input to the cryptographic function of the HSM 130, which produces one or more diversified keys 122 as output. In other embodiments, the server 106 encrypts the master key 118, unique ID 114, and any additional data to generate the diversified keys 122. The resulting diversified keys 122 may correspond to the diversified keys 122 of the contactless card 102. The generated diversified keys 122 are used to decrypt the cryptogram 124 and/or verify the MAC once decrypted. For example, the server 106 may generate a MAC based on the same data as the applet 116, e.g., the sensitive data, the unique ID 114, the counter 120, and/or any additional data. If the MAC generated by the server 106 matches the decrypted MAC in the cryptogram 124, the server 106 may verify or otherwise successfully authenticate the cryptogram 124.

[0061] Regardless of the decryption technique used, the authentication application 138 and/or the HSM 130 may successfully decrypt the cryptogram 124 and verify the MAC, thereby verifying or authenticating the cryptogram 124. If the decryption and/or MAC verification is successful, the authentication application 138 and/or the HSM 130 may generate and transmit a notification indicative that the user 110 has been authenticated. If the authentication application 138 is unable to decrypt the cryptogram 124 (and/or is unable to verify the MAC) the authentication application 138 does not validate the cryptogram 124. In such an example, the authentication application 138 determines to refrain from generating and transmitting a notification. The authentication application 138 may transmit an indication of the failed decryption and/or verification to the computing device 104.

[0062] In one or more embodiments, the user 110 may have one or more printable document 144 associated with the account 142. The user 110 may desire to print, i.e., make physical copies of the printable document 144. Alternatively, or in addition, the user 110 may have to print some of the material as per requirements of the account provider. In some embodiments,

the one or more printable document 144 may include sensitive and/or secure information that the user 110 may not want to, or may not be permitted to, print unless the printer being used is a trusted secure device. For example, the printable document 144 may include checks, balance statements, boarding passes, coupons, paystubs, confidential/privileged documents, or any other documents that include information that is deemed to be sensitive, privileged, secret, personal, etc., either by the user 110 or the account provider. Hence, printing the one or more printable document 144 is restricted to a trusted printer, such as the printer 108. In other embodiments, the user 110 may not have access to a private printer (e.g., printer at home) and hence, may be printing the printable document 144 (with/without sensitive, privileged, secret, personal, etc., information) at the printer 108, which is a public printer.

[0063] Accordingly, a technical challenge exists of creating and executing a secure printing (print job) of the printable document 144 from the account 142, where the printed material is only available upon authentication of the user 110. Further, the technical challenge is to verify that the user 110 is physically present at the printer 108 when the printable document 144 are printed. Embodiments described herein address such technical challenges. The authentication and the verification of the user 110 using the contactless card 102 is used to ensure that the authorized user 110 is physically present at the printer 108 when the requested printable document 144 are being printed. In some embodiments, a combination of the contactless card 102, the computing device 104, and the printer 108 is used by the server 106 to verify that the user 110 is who he/she claims to be before releasing the printable document 144. In some embodiments, the printable document 144 are released for printing by the printer 108 upon performing the authentication and verification of the user 110.

[0064] In some embodiments, to process the printing of the printable document 144, the system 100 includes a print engine 146. The print engine 146 is shown as a part of the server 106, however, in other embodiments, the print engine 146 can be part of some other component of the system 100 or may be a separate component by itself. The print engine 146 may be accessible to the user 110 via the account application 136 only when the user 110 has been authenticated using the contactless card 102. Alternatively, or in addition, the user 110 may request to print one or more of the printable documents 144 only upon successful authentication using the contactless card 102. In other words, the user 110 has to create a secure authenticated session with the server 106 to request printing the printable document 144.

[0065] The user 110, via the account application 136, can select one or more documents to be printed from the printable document 144. In some embodiments, the printable document 144 have already been generated, e.g., monthly statements, transaction history, etc. Alternatively, or in addition, the user 110 selects a type or description of document to be printed. Subsequently, a corresponding printable document 144 is dynamically generated based on the selection and information provided by the user 110. In some embodiments, the printable document 144 can be generated as soon as the user 110 makes the selection and provides corresponding information. Alternatively, in some embodiments, the printable document 144 is dynamically generated upon the user 110 verifying his/her presence at the printer 108.

[0066] The server 106 can add one or more of the printable documents 144 selected/generated for printing to a print queue 148. In some embodiments, the print queue 148 is specific to the user 110 with the contactless card 102. Alternatively, or in addition, the print queue 148 is specific to the account 142, which may have more than one contactless card 102 associated with it. Thus, a first contactless card 102 associated with the account 142 may be used to make a request to print one or more printable documents 144. Subsequently, a second contactless card 102, which is also associated with the same account 142, is used to release the printable documents 144 at the printer 108. Adding a printable document 144 to the print queue 148 may include associating the printable document 144 with additional information, such as information to verify the user 110 to be authenticated to receive printed copies of the printable document 144.

[0067] In some embodiments, the printer 108 is designated to print the requested printable document 144 based on the printer 108 being a secure printer 108. A secure printer 108 may be a printer device that is identified by a print engine 146 as a trusted printer device. The printer 108 may be identified as a trusted device based on the printer 108 being connected to the print engine 146 via a secure communication link. Alternatively, or in addition, the printer 108 may include one or more modules and/or trust certificates (not shown) that identify the printer 108 as a trusted device.

[0068] Further, in some embodiments, the printer 108 may be identified and designated to print the requested printable document 144 based on one or more attributes of the user 110. For example, the printer 108 may be selected based on a location of the user 110, where the location is automatically identified based on the computing device 104. The location is automatically identified based on a position sensor (not shown) equipped on the computing

device 104. The printer 108 may be selected by the server 106 or by the print engine 146. Alternatively, or in addition, the printer 108 may be selected based on a location input by the user 110 via a user interface of the account application 136. Alternatively, or in addition, the attributes of the user 110 used to select the printer 108 may include a historic pattern of printers that the user 110 has previously used and preferred. The preference may be based on an input provided by the user 110. Further, the printer 108 may be selected based on a status of the user 110 as indicated by the contactless card 102. For example, the status can indicate a level of the account 142, e.g., a silver member, a gold member, a diamond member, etc. Any other tiered rating may be used to provide the status levels. The status level may be decided on several factors, such as card expenses, card usage, organizational position, card age, card fees, etc., of the user 110.

[0069] In one or more embodiments, the printer 108 is a self-service printer, without any human operator. Accordingly, the technical challenges addressed by embodiments described herein are self-service-kiosk centric, and as such, necessarily require a technical or technological solution. In other words, verifying and/or authenticating the user 110 at the printer 108 has to be done electronically or digitally using one or more computing devices. As such, technical solutions provided by embodiments described herein are rooted in the technical field of self-service printers and provide improvements to the self-service printers by facilitating such devices to authenticate and/or verify the user 110 who has arrived to collect copies of the printable documents 144. Embodiments described herein further provide a practical application of preventing fraudulent activity by enabling a self-service printer to authenticate and verify an identity of the receiving user 110 prior to printing copies of the printable documents 144 for the user 110.

[0070] In some embodiments, the printer 108 includes an account application 136. The account application 136 may be substantively similar to the account application 136 on the computing device 104. Alternatively, in some embodiments, the account application 136 may be a limited version of the account application 136 on the computing device 104. For example, the account application 136 on the printer 108 may only have features associated with releasing and printing the printable documents 144, and none of the features associated with selecting the printable documents 144. Accordingly, the account application 136 on the printer 108 may allow the user 110 to access and print the printable documents 144 that s/he has already selected for printing.

[0071] In some embodiments, the printer 108 includes the communications interface 126 to facilitate the printer 108 to authenticate the identity of the user 110 via the contactless card 102 as described herein. The communications interface 126 can facilitate the account application 136 to communicate with the contactless card 102, for example, to obtain the cryptogram 124 from the contactless card 102. The communications interface 126 can further facilitate other types of communications by the printer 108, such as with the server 106, the computing device 104, etc. Such communications can include wired and/or wireless communications. The communications interface 126 of the printer 108 may also include machine-readable code scanner, for example, to read machine-readable codes, such as barcodes, quick-response (QR) codes, etc.

[0072] In some embodiments, one or more components of the communications interface 126 may be externally equipped onto the printer 108. For example, the communications interface 126 may be part of a separate device that is coupled with the printer 108 to facilitate the printer 108 to communicate using the one or more protocols supported by the communications interface 126.

[0073] FIG. 2A is a schematic 300a illustrating an embodiment where a contactless card 102 is tapped to a computing device 104, e.g., to obtain the cryptogram 124. As stated, when the contactless card 102 is tapped to the computing device 104, the applet 116 may generate a cryptogram (e.g., the cryptogram 124). The cryptogram 124 and any other data (e.g., unencrypted unique ID 114) may be included in a data package, such as an NDEF file, that is read by the computing device 104. The computing device 104 may then transmit the cryptogram 124 (and other data) to the server 106 for verification (e.g., decryption and/or MAC verification) as described herein.

[0074] FIG. 2B is a schematic 300b illustrating an embodiment where the server 106 verified the cryptogram 124 generated by the contactless card 102 (e.g., see FIG. 2A). Based on the verification, the server 106 may create a one-time password (OTP) 202. The OTP 202 can be a pseudo-random code, for example. In some embodiments, the OTP 202 is generated based on one or more attributes of the account 142 associated with the contactless card 102. The server 106 may then transmit the OTP 202 to the account application 136. As shown, the account application 136 may then display the OTP 202 on the display of the computing device 104. The OTP 202 can include a string of characters. In some embodiments, the OTP 202 includes or is represented as a matrixed code, which is machine-readable. Doing so allows the OTP 202 to be

scanned by a code reader. The OTP 202 is used in some embodiments for a multi-factor authentication to verify the user 110.

[0075] FIG. 3 depicts an example scenario of usage of the system 100. Consider the scenario where the user 110 accesses her bank account 142 via her mobile computing device 104 to select and print a printable document 144. The selected printable document 144 contains sensitive information and has to be printed at a secure printer 108. The user 110 prefers the printer 108 used for the printing to be closer to her work location, rather than her home location. It is understood that the scenario is just one example scenario that is being used as an illustration to describe embodiments herein. The scenario is non-limiting and technical solutions provided by embodiments described herein can be used in several other scenarios in the context of a bank account, or any other type of account.

[0076] FIG. 4 illustrates an embodiment of a method, logic flow, or routine 400. The routine 400 may be representative of some or all of the operations executed by one or more embodiments described herein. For example, the routine 400 may include some or all of the operations to complete a print-request to print one or more printable documents 144 at a self-service printer 108 in a secured manner as described herein. Embodiments are not limited in this context.

[0077] The routine 400 is described in the context of the example scenario illustrated in FIG. 3. It is understood that the scenario is just one example scenario that is being used as an illustration to describe embodiments herein. The scenario is non-limiting and technical solutions provided by embodiments described herein can be used in several other scenarios in the context of a bank account, or any other type of account. In some embodiments, the operations described herein may be described as being performed by the server 106. However, in other embodiments, the operations can be performed by the server 106, a system including one or more servers, or any other type of device.

[0078] In block 402, the server 106 receives a first request to setup a first authenticated session associated with the account 142. The first request is received from the computing device 104, particularly from the account application 136. The account application 136 generates the first request when the user 110 logs into the account application 136. In some embodiments, the user 110 may login to the account application 136 by providing one or more authentication credentials. Alternatively, or in addition, the user 110 may have to verify her identity using the contactless card 102, as described herein. For example, the user 110 may be

instructed to bring the contactless card 102 within a predetermined vicinity or range of the computing device 104. Once the contactless card 102 and the computing device 104 are within communication range for NFC based communication, as described in detail herein, the account application 136 will perform an authentication procedure based on the cryptogram 124 from the contactless card 102, which is transmitted to the server 106 for verification. The description of the authentication procedure is not repeated here for brevity.

[0079] In block 404, the server 106 establishes the first authenticated session in response to authenticating the account 142 being accessed via the computing device 104. In some embodiments, the user 110 can avail of printing services for the account 142 only if such an authenticated session is established. For example, if the user 110 only uses authentication credentials to login (first level security) and does not provide the contactless card 102 for further verification (second level security), the user 110 may avail of a limited subset of features of the account 142. Such a subset of features may not include the printing services offered by the account 142. In other embodiments, the user 110 may avail of the printing services even at the first level security.

[0080] In block 406, the server 106 receives, during the first authenticated session, a print-request to print a printable document 144 associated with the account 142. For example, the user 110 may select to print bank statements for specific month(s). Alternatively, or in addition, the user 110 may select to print a receipt of a one or more transactions. Alternatively, or in addition, the user 110 may select to print a check, such as a cashier's check. It is understood that the user 110 may not be limited to the example printable documents 144 listed herein.

[0081] In block 408, the server 106, adds a print queue 148 to the print queue 148, the print job is for the selected printable documents 144. The print queue 148 may include all of the selected printable documents 144. Alternatively, in some embodiments, each printable document 144 may be added as a separate print queue 148 to the print queue 148. A print queue 148 for a printable document 144 may include an identifier and an image of the one or more printable documents 144 in the print queue 148. The image of the printable document 144 is what is printed by the printer 108 to create a physical copy of the printable document 144.

[0082] In some embodiments, adding the print queue 148 includes creating a print queue 148 in the print engine 146 for the account 142. In some embodiments, the print queue 148 may be associated with the account 142. The server 106 creates the print queue 148 for the account 142 using an application programming interface (API) for the print engine 146. Creating the print

queue 148 may include executing one or more commands specifying an identifier of the account 142. Once the print queue 148 is created, the print queue 148 is added to the print queue 148. In some embodiments, the print queue 148 has a predetermined expiration, e.g., 24 hours, 48 hours, or any other such duration. After expiration of the duration, the print queue 148 is deleted by the print engine 146 from the print queue 148. In some embodiments, the print engine 146 may generate a notification to the user 110 indicating that the print queue 148 is about to expire. Such a notification may be provided via the account application 136 on the computing device 104. The notification may be provided at a predetermined duration before the preset expiration, for example, 4 hours prior, 8 hours prior, 1 hour prior, etc. The user 110 may respond to such an expiration notification by renewing the print queue 148. The renewal may be for the same or a different predetermined expiration. In some embodiments, such a renewal process may be limited only to a predetermined number of times, e.g., 3, 5, etc.

[0083] In some embodiments, the print queue 148 may have a predetermined expiration. If the print queue 148 is empty, i.e., has no print queues 148, the print engine 146 may remove (delete) the print queue 148. Otherwise, the print engine 146 delays removal of the print queue 148 that is not empty by a predetermined duration.

[0084] The print queue 148 may be accessible when the account 142 is accessed. The user 110 may access the print queue 148 via the account application 136. In some embodiments, the user 110 can see, edit, delete one or more print queues 148 in the print queue 148 until the print queues 148 are released for printing at the printer 108.

[0085] In some embodiments, at the time of adding the print queue 148 to the print queue 148, the user 110 may select the printer 108. The selection of the printer 108 depends on one or more attributes as described herein. In some embodiments, selecting the printer 108 may depend on the type of the one or more printable documents 144 selected. For example, if a selected printable document 144 is of a particular type, the printer 108 may have to have the authority and/or capability to print that type of printable document 144. For example, the type of the printable document 144 may be but not limited to a report, an account statement, a transaction history, a check, a money transfer instruction, a form, a letter, an offer, or a combination thereof. Of these, printing a check may require a higher level of trust than an account statement, for example. Accordingly, only a limited number of printers 108 may have the capability and resources (e.g., special paper, special ink, special print head, etc.) to print such a type of printable document 144 (e.g., check). Therefore, only the printer 108 from such a

limited set of printers 108 may be selected. In another case, for the printable document 144, such as the account statement, which may not require such a higher level of trust, any printer 108 that provides the verified printing can be used.

[0086] The printer 108 may be selected from one or more self-service printers that are installed at one or more locations of the account provider. For example, such self-service printers may be placed at bank locations, pharmacies, grocery stores, gas stations, printing-service stores, airports, railway stations, or any other locations selected by the account provider.

[0087] In some embodiments, the account application 136 displays to the user 110 a list of printers 304 that can be used for printing the selected printable documents 144 based on the types of the one or more printable documents 144 selected. The displayed list of printers 304 may be filtered and/or sorted according to one or more attributes of the user 110. For example, the displayed list of printers 304 may be sorted according to the user's recent visits and/or transactions to the one or more printers. Alternatively, the displayed list of printers 304 may be sorted according to a distance, travel time, or other such location-based information based on the present location of the user 110. The present location of the user 110 may be determined using a position sensor of the computing device 104. In some embodiments, the user 110 may manually filter, sort, and expand the list of printers 304 suggested via the user interface.

[0088] In some embodiments, the user 110 may not select the printer 108 when the print job 302 is created and added into the print queue 148. Instead, the user 110 may proceed to any one of printers without a selection to release the printable documents 144 that are queued in the print queue 148. Alternatively, the user 110 proceeds to a selected printer 108 to release the printable documents 144 that are queued in the print queue 148.

[0089] In block 410 of the routine 400 the server 106 receives a request to initiate a second authenticated session associated with the account 142. The second request may be received from the printer 108 at which the user 110 desires to release the printable documents 144 that are queued. In some embodiments, the printer 108 may have the account application 136. In some embodiments, the account application 136 of the printer 108 provides a limited set of features compared to the account application 136 available on the computing device 104.

[0090] In response to receiving the request, the server 106 prompts the printer 108 to perform the authentication procedure described herein. Accordingly, the printer 108 requests the user 110 to tap the contactless card 102 to the printer 108 or a designated location to authenticate

his/her identity. The account application 136 obtains the cryptogram 124 from the contactless card 102 via the communications interface 126 of the printer 108. In some embodiments, the same contactless card 102 that was used to initiate the first authenticated session has to be used to initiate the second authenticated session. Alternatively, a second contactless card 102 (different from the contactless card 102 used to initiate the first authenticated session) may be used to initiate the second authenticated session, where the second contactless card 102 is also associated with the account 142.

[0091] The account application 136 transmits the cryptogram 124 obtained from the presented contactless card 102 to the server 106 for verification. If the authentication of the identity of the user 110 fails, the printer 108 notifies the user 110 that the authentication failed. Accordingly, the print jobs 302 in the print queue 148 are not accessible to the printer 108, and the printable documents 144 cannot be printed.

[0092] In some embodiments, the printer 108 may not have the capability to receive and/or transmit the cryptogram 124 from the contactless card 102. In such cases, in response to the request for the second authenticated session, the server 106 prompts the computing device 104 to perform the authentication procedure using the contactless card 102. Upon completion of the authentication procedure, the computing device 104 receives the OTP 202 from the server 106. The OTP 202 is entered into the printer 108 to verify the identity of the user 110. In some embodiments, the OTP 202 is entered manually, for example, using a keyboard or another input device. Alternatively, the OTP 202 may be electronically received by the printer 108 from the computing device 104, for example, using a machine-readable code reader, such as a barcode scanner, a QR-code scanner, a camera, etc. The code reader (not shown) of the printer 108 scans the machine-readable portion of the OTP 202. Upon receiving the OTP 202 from the printer 108, the server 106 completes authenticating the user 110 and deems that the verified user 110 is requesting the release of the printable documents 144 at the printer 108.

[0093] In some embodiments, the authentication used to initiate the second authenticated session may be different from the authentication used to initiate the first authenticated session. For example, authenticating the account 142 in response to the first request for the first authenticated session from the computing device 104 a first authentication routine is used. The first authentication routine may be based only on authentication credentials, without using the contactless card 102. For example, the first authentication routine may be based on one or more settings of the account application 136 stored on the computing device 104. The authenticating

of the account 142 by the printer 108 may use a second authentication routine, different from the first authentication routine. This may be because the computing device 104 may be a trusted private device of the user 110 that the user 110 has registered with the account 142 and has been using over a certain duration. In contrast, the printer 108 may be a public device, and therefore not as secure or trusted as the computing device 104. Therefore, a higher level of authentication may be used to authenticate the second request compared to the level of authentication used to authenticate the first request. Accordingly, the second authentication routine may use the contactless card 102 to enhance the security.

[0094] In block 412, the server, initiates the second authenticated session in response to successfully authenticating the account 142 at the printer 108. The server 106 may notify the print engine 146 to release the print queue 148 associated with the account 142 of the verified user 110 to the printer 108. Further, in block 414, the print engine 146 releases the print queue 148 associated with the account 142 to the printer 108. In some embodiments, the print engine 146 and/or the server 106 verifies that the printer 108 is authorized to print the printable document 144 based on the type of the printable documents 144. Additionally, or alternatively, the print engine 146 and/or the server 106 may verify that the printer 108 is capable to print the printable documents 144.

[0095] In some embodiments, such verification may include checking that the printer 108 has the resources available to print the selected printable documents 144. Resources checked may include but are not limited to ink, paper, printer head, etc. The resources are checked based on the type of the printable documents 144. For example, if one of the printable documents 144 requires a particular type of resource, then it is verified that the printer 108 has the particular types of resources available.

[0096] Accordingly, the printer 108 receives the print jobs 302 from the print queue 148. In block 416, the printer 108 prints the printable documents 144 from the print jobs 302. In some embodiments, the printer 108 performs the authentication procedure using the contactless card 102 after completing one or more print jobs 302. In some embodiments, the printer 108 performs the authentication procedure using the contactless card 102 after printing one or more printable documents 144. In this way, the printer 108 ensures that the user 110 is still present to collect the printed copies of the printable documents 144 being printed by the printer 108.

[0097] FIG. 5 illustrates an embodiment of a method, logic flow, or routine 500. The routine 500 may be representative of some or all of the operations executed by one or more

embodiments described herein. For example, the routine 500 may include some or all of the operations to select and print one or more printable documents 144 at a self-service printer 108 in a secured manner as described herein. Embodiments are not limited in this context. In some embodiments, the operations described herein may be described as being performed by a particular device. However, in other embodiments, the operations can be performed by any of the devices described herein, or a combination thereof.

[0098] In block 502, the user 110 selects via the computing device 104, for printing, a printable document 144 associated with the account 142. The user 110 selects the printable document 144 from a several printable documents 144 selectable from the account application 136. The user can select the printable document 144 via the account application 136 only upon successful authentication of his/her identity. The authentication may be performed using a limited authentication, for example, using the authentication credentials of the user 110 only (without the contactless card 102). In some embodiments, the authentication is performed using the contactless card 102.

[0099] In block 504, upon selection of the printable document 144, a list of printers 304 for printing the selected printable document 144 is generated and displayed. The list of printers 304 may be generated by the computing device 104. In some embodiments, the list of printers 304 may be generated by the server 106. The list of printers 304 is generated based on a type of the selected printable document 144. The type of the printable document 144 may be one of a report, an account statement, a transaction history, a check, a money transfer instruction, a form, a letter, an offer, or a combination thereof. In some embodiments, the type of the selected printable document 144 may be privileged and non-privileged. Based on the type of the printable document 144, a printer 108 may or may not be permitted to print the printable document 144. For example, if the type of the printable document 144 is privileged, then only a subset of the printers 108 can be used to print that printable document 144. Whereas, in case of a non-privileged printable document 144, any printer 108 may be used. The subset of printers for the privileged printable document 144 may have additional resources compared to other printers. For example, the subset of printers may have special ink, special paper, special printer heads, additional security, end-to-end encryption, communications interface 126, etc.

[0100] Further, the list of printers 304 may be generated based on other attributes, such as a location of the user 110. The location may be determined based on the computing device 104, in some embodiments. Alternatively, the user 110 may specify a target location, and the list of

printers 304 is generated based on the target location. For example, the list of printers 304 includes first N closest printers that are authorized to print the selected printable document 144. Alternatively, the list of printers 304 includes printers that are authorized to print the selected printable document 144 and within a certain predetermined distance, travel time, of the target location. Other filters may be used to generate the list of printers 304.

[0101] The list of printers 304 is displayed to the user 110 via the account application 136. The list of printers 304 may be selectable in some embodiments.

[0102] In block 506, the user selects from the list of printers 304, the printer 108 to print the printable document 144. The user proceeds to the selected printer 108.

[0103] In block 508, the computing device 104 provides, an authentication code (OTP 202) for the user to access the printer 108 to print the printable document 144. The authentication code is provided by the server 106 via the computing device 104 in response to the user 110 requesting the server 106 to release the printable document 144 to the printer 108. The user 110 may request such a release of the printable document 144 via the printer 108, for example, using the account application 136 of the printer 108. The server 106, in response, prompts the user 110 via the computing device 104 to verify his/her identity using the contactless card 102. The authentication procedure described herein is performed based on the computing device 104 accessing the cryptogram 124 from the contactless card 102 and transmitting the cryptogram 124 to the server 106 for verification. The server 106 provides the authentication code, i.e., OTP 202 to the computing device 104 in response to successful verification/authentication.

[0104] In block 510, the printer 108 receives and prints the printable document 144 in response to receiving the authentication code from the computing device 104. The authentication code can be scanned by the printer 108 from the computing device 104 using a scanner, such as a barcode scanner, camera, QR-code scanner, an NFC reader, or any other machine-readable code scanner. Alternatively, the user 110 enters the authentication code from the computing device manually into the printer 108. The printer 108 communicates the authentication code to the server 106, which releases the printable document 144 to the printer 108 upon the authentication code matching the generated authentication code.

[0105] FIG. 6 illustrates an embodiment of a logic flow, or routine 600. The routine 600 may be representative of some or all of the operations executed by one or more embodiments described herein. For example, the routine 600 may include some or all of the operations to perform an authentication procedure, for example, to enable the user 110 to access one or more

features of the account 142. Embodiments are not limited in this context. In some embodiments, the operations described herein may be described as being performed by a particular device. However, in other embodiments, the operations can be performed by any of the devices described herein, or a combination thereof.

[0106] In block 602, the server 106 receives from an account application 136, a request to access a feature of the account 142. The feature may be to create a print-request, to release the print queue 148, etc. The account application 136 may be executing on the computing device 104, the printer 108, etc. The received request includes or is associated with the cryptogram 124. The cryptogram 124 is obtained by the account application 136 from the contactless card 102.

[0107] In block 604, the server 106 may decrypt the cryptogram 124 by generating one or more diversified keys 122 based on the master key 118 and a counter 120. The server 106 may further verify the cryptogram 124, e.g., determine that a MAC generated by the server 106 matches a MAC in the decrypted cryptogram 124.

[0108] In block 606, the server 106 may generate an authorization based on the successful decryption and verification. The authorization may generally indicate that the requested access to the feature of the account 142 is to be permitted.

[0109] In block 608, the server 106 transmits the authorization to the account application 136. The authorization may cause the account application 136 to permit the requested access to the feature. In some embodiments, however, the verification may not be successful, in which case, the account application 136 prohibits the user 110 from accessing the requested feature.

[0110] FIG. 7A is a schematic 700 illustrating an example configuration of a contactless card 102, which may include a payment card, such as a credit card, debit card, or gift card, issued by a service provider as displayed as service provider indicia 706 on the front or back of the contactless card 102. In some examples, the contactless card 102 is not related to a payment card, and may include, without limitation, an identification card. In some examples, the transaction card may include a dual interface contactless payment card, a rewards card, and so forth. The contactless card 102 may include a substrate 708, which may include a single layer, or one or more laminated layers composed of plastics, metals, and other materials. Exemplary substrate materials include polyvinyl chloride, polyvinyl chloride acetate, acrylonitrile butadiene styrene, polycarbonate, polyesters, anodized titanium, palladium, gold, carbon, paper, and biodegradable materials. In some examples, the contactless card 102 may have

physical characteristics compliant with the ID-1 format of the ISO/IEC 7816 standard, and the transaction card may otherwise be compliant with the ISO/IEC 14443 standard. However, it is understood that the contactless card 102 according to the present disclosure may have different characteristics, and the present disclosure does not require a transaction card to be implemented in a payment card.

[0111] The contactless card 102 may also include identification information 710 displayed on the front and/or back of the card, and a contact pad 712. The contact pad 712 may include one or more pads and be configured to establish contact with another client device, such as an ATM, a user device, smartphone, laptop, desktop, or tablet computer via transaction cards. The contact pad may be designed in accordance with one or more standards, such as ISO/IEC 7816 standard, and enable communication in accordance with the EMV protocol. The contactless card 102 may also include processing circuitry, antenna and other components as will be further discussed in FIG. 7B. These components may be located behind the contact pad 712 or elsewhere on the substrate 708, e.g., within a different layer of the substrate 708, and may electrically and physically coupled with the contact pad 712. The contactless card 102 may also include a magnetic strip or tape, which may be located on the back of the card (not shown in FIG. 7A). The contactless card 102 may also include a Near-Field Communication (NFC) device coupled with an antenna capable of communicating via the NFC protocol. Embodiments are not limited in this manner.

[0112] As illustrated in FIG. 7B, the contact pad 712 of contactless card 102 may include processing circuitry 714 for storing, processing, and communicating information, including a processor 716, a memory 112, and one or more communications interface 126. It is understood that the processing circuitry 714 may contain additional components, including processors, memories, error and parity/CRC checkers, data encoders, anticollision algorithms, controllers, command decoders, security primitives and tamperproofing hardware, as necessary to perform the functions described herein.

[0113] The memory 112 may be a read-only memory, write-once read-multiple memory, or read/write memory, e.g., RAM, ROM, and EEPROM, and the contactless card 102 may include one or more of these memories. A read-only memory may be factory programmable as read-only or one-time programmable. One-time programmability provides the opportunity to write once then read many times. A write once/read-multiple memory may be programmed at a point in time after the memory chip has left the factory. Once the memory is programmed, it may not

be rewritten, but it may be read many times. A read/write memory may be programmed and re-programmed many times after leaving the factory. A read/write memory may also be read many times after leaving the factory. In some instances, the memory 112 may be encrypted memory utilizing an encryption algorithm executed by the processor 716 to encrypted data.

[0114] The memory 112 may be configured to store one or more applet 116, one or more counters 120, a unique ID 114, the master key 118, the UDK 702, diversified key 122, and the PAN sequence 704. The one or more applets 116 may comprise one or more software applications configured to execute on one or more contactless cards 102, such as a Java® Card applet. However, it is understood that applets 116 are not limited to Java Card applets, and instead may be any software application operable on contactless cards or other devices having limited memory. The one or more counters 120 may comprise a numeric counter sufficient to store an integer. The unique ID 114 may comprise a unique alphanumeric identifier assigned to the contactless card 102, and the identifier may distinguish the contactless card 102 from other contactless cards 102. In some examples, the unique ID 114 may identify both a customer and an account assigned to that customer.

[0115] The processor 716 and memory elements of the foregoing exemplary embodiments are described with reference to the contact pad 712, but the present disclosure is not limited thereto. It is understood that these elements may be implemented outside of the contact pad 712 or entirely separate from it, or as further elements in addition to processor 716 and memory 112 elements located within the contact pad 712.

[0116] In some examples, the contactless card 102 may comprise one or more antenna(s) 718. The one or more antenna(s) 718 may be placed within the contactless card 102 and around the processing circuitry 714 of the contact pad 712. For example, the one or more antenna(s) 718 may be integral with the processing circuitry 714 and the one or more antenna(s) 718 may be used with an external booster coil. As another example, the one or more antenna(s) 718 may be external to the contact pad 712 and the processing circuitry 714.

[0117] In an embodiment, the coil of contactless card 102 may act as the secondary of an air core transformer. The terminal may communicate with the contactless card 102 by cutting power or amplitude modulation. The contactless card 102 may infer the data transmitted from the terminal using the gaps in the power connection of the contactless card 102, which may be functionally maintained through one or more capacitors. The contactless card 102 may communicate back by switching a load on the coil of the contactless card 102 or load

modulation. Load modulation may be detected in the terminal's coil through interference. More generally, using the antenna(s) 718, processor 716, and/or the memory 112, the contactless card 102 provides a communications interface to communicate via NFC, Bluetooth, and/or Wi-Fi communications.

[0118] As explained above, contactless card 102 may be built on a software platform operable on smart cards or other devices having limited memory, such as JavaCard, and one or more or more applications or applets may be securely executed. Applet 116 may be added to contactless cards to provide a one-time password (OTP) for MFA in various mobile application-based use cases. Applet 116 may be configured to respond to one or more requests, such as near field data exchange requests, from a reader, such as a mobile NFC reader (e.g., of a mobile computing device 104 or point-of-sale terminal) and produce an NDEF message that comprises a cryptographically secure OTP encoded as an NDEF text tag. The NDEF message may include a cryptogram such as the cryptogram 124, and any other data.

[0119] One example of an NDEF OTP is an NDEF short-record layout (SR=1). In such an example, one or more applet 116 may be configured to encode the OTP as an NDEF type 4 well known type text tag. In some examples, NDEF messages may comprise one or more records. The applet 116 may be configured to add one or more static tag records in addition to the OTP record.

[0120] In some examples, the one or more applet 116 may be configured to emulate an RFID tag. The RFID tag may include one or more polymorphic tags. In some examples, each time the tag is read, different cryptographic data is presented that may indicate the authenticity of the contactless card 102. Based on the one or more applet 116, an NFC read of the tag may be processed, the data may be transmitted to a server, such as a server of a banking system, and the data may be validated at the server.

[0121] In some examples, the contactless card 102 and server may include certain data such that the card may be properly identified. The contactless card 102 may include one or more unique identifiers (not pictured). Each time a read operation takes place, the counter 120 may be configured to increment. In some examples, each time data from the contactless card 102 is read (e.g., by a mobile device), the counter 120 is transmitted to the server for validation and determines whether the counter 120 are equal (as part of the validation) to a counter of the server.

[0122] The one or more counter 120 may be configured to prevent a replay attack. For example, if a cryptogram has been obtained and replayed, that cryptogram is immediately rejected if the counter 120 has been read or used or otherwise passed over. If the counter 120 has not been used, it may be replayed. In some examples, the counter that is incremented on the contactless card 102 is different from the counter that is incremented for transactions. The contactless card 102 is unable to determine the application transaction counter 120 since there is no communication between applets 116 on the contactless card 102. In some examples, the contactless card 102 may comprise a first applet 440-1, which may be a transaction applet, and a second applet 440-2. Each applet 440-1 and 440-2 may comprise a respective counter 120.

[0123] In some examples, the counter 120 may get out of sync. In some examples, to account for accidental reads that initiate transactions, such as reading at an angle, the counter 120 may increment but the application does not process the counter 120. In some examples, when the mobile device 10 is woken up, NFC may be enabled and the computing device 104 may be configured to read available tags, but no action is taken responsive to the reads.

[0124] To keep the counter 120 in sync, an application, such as a background application, may be executed that would be configured to detect when the computing device 104 wakes up and synchronize with the server of a banking system indicating that a read that occurred due to detection to then move the counter 120 forward. In other examples, Hashed One Time Password may be utilized such that a window of mis-synchronization may be accepted. For example, if within a threshold of 10, the counter 120 may be configured to move forward. But if within a different threshold number, for example within 10 or 600, a request for performing re-synchronization may be processed which requests via one or more applications that the user tap, gesture, or otherwise indicate one or more times via the user's device. If the counter 120 increases in the appropriate sequence, then it possible to know that the user has done so.

[0125] The key diversification technique described herein with reference to the counter 120, master key 118, UDK 702, and diversified key 122, is one example of encryption and/or decryption a key diversification technique. This example key diversification technique should not be considered limiting of the disclosure, as the disclosure is equally applicable to other types of key diversification techniques.

[0126] During the creation process of the contactless card 102, two cryptographic keys may be assigned uniquely per card. The cryptographic keys may comprise symmetric keys which may be used in both encryption and decryption of data. Triple DES (3DES) algorithm may be

used by EMV, and it is implemented by hardware in the contactless card 102. By using the key diversification process, one or more keys may be derived from a master key based upon uniquely identifiable information for each entity that requires a key.

[0127] In some examples, to overcome deficiencies of 3DES algorithms, which may be susceptible to vulnerabilities, a session key may be derived (such as a unique key per session) but rather than using the master key, the unique card-derived keys and the counter may be used as diversification data. For example, each time the contactless card 102 is used in operation, a different key may be used for creating the message authentication code (MAC) and for performing the encryption. This results in a triple layer of cryptography. The session keys may be generated by the one or more applets and derived by using the application transaction counter with one or more algorithms (as defined in EMV 4.3 Book 2 A1.3.1 Common Session Key Derivation).

[0128] Further, the increment for each card may be unique, and assigned either by personalization, or algorithmically assigned by some identifying information. For example, odd numbered cards may increment by 2 and even numbered cards may increment by 5. In some examples, the increment may also vary in sequential reads, such that one card may increment in sequence by 1, 3, 5, 2, 2, ... repeating. The specific sequence or algorithmic sequence may be defined at personalization time, or from one or more processes derived from unique identifiers. This can make it harder for a replay attacker to generalize from a small number of card instances.

[0129] The authentication message may be delivered as the content of a text NDEF record in hexadecimal ASCII format. In another example, the NDEF record may be encoded in hexadecimal format.

[0130] FIG. 8 illustrates an NDEF short-record layout (SR=1) data structure 800 according to an example embodiment. One or more applets 116 may be configured to encode an OTP as an NDEF type 4 well known type text tag. In some examples, NDEF messages may comprise one or more records. The applets may be configured to add one or more static tag records in addition to the OTP record. Exemplary tags include, without limitation, Tag type: well known type, text, encoding English (en); Applet ID: D2760000850101; Capabilities: read-only access; Encoding: the authentication message may be encoded as ASCII hex; type-length-value (TLV) data may be provided as a personalization parameter that may be used to generate the NDEF message. In an embodiment, the authentication template may comprise the first record, with a

well-known index for providing the actual dynamic authentication data. The data structure 800 may include a cryptogram such as cryptogram 124 or cryptogram 202, and any other data provided by the applet 116.

[0131] FIG. 9 illustrates an embodiment of an exemplary computer architecture 900 suitable for implementing various embodiments as previously described. In one embodiment, the computer architecture 900 may include or be implemented as part of system 100.

[0132] As used in this application, the terms “system” and “component” are intended to refer to a computer-related entity, either hardware, a combination of hardware and software, software, or software in execution, examples of which are provided by the exemplary computing computer architecture 900. For example, a component can be, but is not limited to being, a process running on a processor, a processor, a hard disk drive, multiple storage drives (of optical and/or magnetic storage medium), an object, an executable, a thread of execution, a program, and/or a computer. By way of illustration, both an application running on a server and the server can be a component. One or more components can reside within a process and/or thread of execution, and a component can be localized on one computer and/or distributed between two or more computers. Further, components may be communicatively coupled to each other by various types of communications media to coordinate operations. The coordination may involve the uni-directional or bi-directional exchange of information. For instance, the components may communicate information in the form of signals communicated over the communications media. The information can be implemented as signals allocated to various signal lines. In such allocations, each message is a signal. Further embodiments, however, may alternatively employ data messages. Such data messages may be sent across various connections. Exemplary connections include parallel interfaces, serial interfaces, and bus interfaces.

[0133] The computer architecture 900 includes various common computing elements, such as one or more processors, multi-core processors, co-processors, memory units, chipsets, controllers, peripherals, interfaces, oscillators, timing devices, video cards, audio cards, multimedia input/output (I/O) components, power supplies, and so forth. The embodiments, however, are not limited to implementation by the computing computer architecture 900.

[0134] As shown in FIG. 9, the computer architecture 900 includes a computer 912 comprising a processor 902, a system memory 904 and a system bus 906. The processor 902

can be any of various commercially available processors. The computer 912 may be representative of the computing device 104 and/or the server 106.

[0135] The system bus 906 provides an interface for system components including, but not limited to, the system memory 904 to the processor 902. The system bus 906 can be any of several types of bus structure that may further interconnect to a memory bus (with or without a memory controller), a peripheral bus, and a local bus using any of a variety of commercially available bus architectures. Interface adapters may connect to the system bus 906 via slot architecture. Example slot architectures may include without limitation Accelerated Graphics Port (AGP), Card Bus, (Extended) Industry Standard Architecture ((E)ISA), Micro Channel Architecture (MCA), NuBus, Peripheral Component Interconnect (Extended) (PCI(X)), PCI Express, Personal Computer Memory Card International Association (PCMCIA), and the like.

[0136] The computer architecture 900 may include or implement various articles of manufacture. An article of manufacture may include a computer-readable storage medium to store logic. Examples of a computer-readable storage medium may include any tangible media capable of storing electronic data, including volatile memory or non-volatile memory, removable or non-removable memory, erasable or non-erasable memory, writeable or re-writeable memory, and so forth. Examples of logic may include executable computer program instructions implemented using any suitable type of code, such as source code, compiled code, interpreted code, executable code, static code, dynamic code, object-oriented code, visual code, and the like. Embodiments may also be at least partly implemented as instructions contained in or on a non-transitory computer-readable medium, which may be read and executed by one or more processors to enable performance of the operations described herein.

[0137] The system memory 904 may include various types of computer-readable storage media in the form of one or more higher speed memory units, such as read-only memory (ROM), random-access memory (RAM), dynamic RAM (DRAM), Double-Data-Rate DRAM (DDRAM), synchronous DRAM (SDRAM), static RAM (SRAM), programmable ROM (PROM), erasable programmable ROM (EPROM), electrically erasable programmable ROM (EEPROM), flash memory, polymer memory such as ferroelectric polymer memory, ovonic memory, phase change or ferroelectric memory, silicon-oxide-nitride-oxide-silicon (SONOS) memory, magnetic or optical cards, an array of devices such as Redundant Array of Independent Disks (RAID) drives, solid state memory devices (e.g., USB memory, solid state drives (SSD) and any other type of storage media suitable for storing information. In the

illustrated embodiment shown in FIG. 9, the system memory 904 can include non-volatile 908 and/or volatile 910. A basic input/output system (BIOS) can be stored in the non-volatile 908.

[0138] The computer 912 may include various types of computer-readable storage media in the form of one or more lower speed memory units, including an internal (or external) hard disk drive 914, a magnetic disk drive 916 to read from or write to a removable magnetic disk 918, and an optical disk drive 920 to read from or write to a removable optical disk 922 (e.g., a CD-ROM or DVD). The hard disk drive 914, magnetic disk drive 916 and optical disk drive 920 can be connected to the system bus 906 by an HDD interface 924, and FDD interface 926 and an optical disk drive interface 928, respectively. The HDD interface 924 for external drive implementations can include at least one or both of Universal Serial Bus (USB) and IEEE 1394 interface technologies.

[0139] The drives and associated computer-readable media provide volatile and/or nonvolatile storage of data, data structures, computer-executable instructions, and so forth. For example, a number of program modules can be stored in the drives and non-volatile 908, and volatile 910, including an operating system 930, one or more applications 932, other program modules 934, and program data 936. In one embodiment, the one or more applications 932, other program modules 934, and program data 936 can include, for example, the various applications and/or components of the system 100.

[0140] A user can enter commands and information into the computer 912 through one or more wire/wireless input devices, for example, a keyboard 938 and a pointing device, such as a mouse 940. Other input devices may include microphones, infra-red (IR) remote controls, radiofrequency (RF) remote controls, game pads, stylus pens, card readers, dongles, fingerprint readers, gloves, graphics tablets, joysticks, keyboards, retina readers, touch screens (e.g., capacitive, resistive, etc.), trackballs, track pads, sensors, styluses, and the like. These and other input devices are often connected to the processor 902 through an input device interface 942 that is coupled to the system bus 906 but can be connected by other interfaces such as a parallel port, IEEE 1394 serial port, a game port, a USB port, an IR interface, and so forth.

[0141] A monitor 944 or other type of display device is also connected to the system bus 906 via an interface, such as a video adapter 946. The monitor 944 may be internal or external to the computer 912. In addition to the monitor 944, a computer typically includes other peripheral output devices, such as speakers, printers, and so forth.

[0142] The computer 912 may operate in a networked environment using logical connections via wire and/or wireless communications to one or more remote computers, such as a remote computer(s) 948. The remote computer(s) 948 can be a workstation, a server computer, a router, a personal computer, portable computer, microprocessor-based entertainment appliance, a peer device or other common network node, and typically includes many or all the elements described relative to the computer 912, although, for purposes of brevity, only a memory and/or storage device 950 is illustrated. The logical connections depicted include wire/wireless connectivity to a local area network 952 and/or larger networks, for example, a wide area network 954. Such LAN and WAN networking environments are commonplace in offices and companies, and facilitate enterprise-wide computer networks, such as intranets, all of which may connect to a global communications network, for example, the Internet.

[0143] When used in a local area network 952 networking environment, the computer 912 is connected to the local area network 952 through a wire and/or wireless communication network interface or network adapter 956. The network adapter 956 can facilitate wire and/or wireless communications to the local area network 952, which may also include a wireless access point disposed thereon for communicating with the wireless functionality of the network adapter 956.

[0144] When used in a wide area network 954 networking environment, the computer 912 can include a modem 958, or is connected to a communications server on the wide area network 954 or has other means for establishing communications over the wide area network 954, such as by way of the Internet. The modem 958, which can be internal or external and a wire and/or wireless device, connects to the system bus 906 via the input device interface 942. In a networked environment, program modules depicted relative to the computer 912, or portions thereof, can be stored in the remote memory and/or storage device 950. It will be appreciated that the network connections shown are exemplary and other means of establishing a communications link between the computers can be used.

[0145] The computer 912 is operable to communicate with wire and wireless devices or entities using the IEEE 802 family of standards, such as wireless devices operatively disposed in wireless communication (e.g., IEEE 802.11 over-the-air modulation techniques). This includes at least Wi-Fi (or Wireless Fidelity), WiMax, and Bluetooth™ wireless technologies, among others. Thus, the communication can be a predefined structure as with a conventional network or simply an ad hoc communication between at least two devices. Wi-Fi networks use radio technologies called IEEE 802.11 (a, b, g, n, ac, ax, etc.) to provide secure, reliable, fast

wireless connectivity. A Wi-Fi network can be used to connect computers to each other, to the Internet, and to wire networks (which use IEEE 802.3-related media and functions).

[0146] The various elements of the devices as previously described with reference to figures herein may include various hardware elements, software elements, or a combination of both. Examples of hardware elements may include devices, logic devices, components, processors, microprocessors, circuits, processors, circuit elements (e.g., transistors, resistors, capacitors, inductors, and so forth), integrated circuits, application specific integrated circuits (ASIC), programmable logic devices (PLD), digital signal processors (DSP), field programmable gate array (FPGA), memory units, logic gates, registers, semiconductor device, chips, microchips, chip sets, and so forth. Examples of software elements may include software components, programs, applications, computer programs, application programs, system programs, software development programs, machine programs, operating system software, middleware, firmware, software modules, routines, subroutines, functions, methods, procedures, software interfaces, application program interfaces (API), instruction sets, computing code, computer code, code segments, computer code segments, words, values, symbols, or any combination thereof. However, determining whether an embodiment is implemented using hardware elements and/or software elements may vary in accordance with any number of factors, such as desired computational rate, power levels, heat tolerances, processing cycle budget, input data rates, output data rates, memory resources, data bus speeds and other design or performance constraints, as desired for a given implementation.

[0147] One or more aspects of at least one embodiment may be implemented by representative instructions stored on a machine-readable medium which represents various logic within the processor, which when read by a machine causes the machine to fabricate logic to perform the techniques described herein. Such representations, known as “IP cores,” may be stored on a tangible, machine readable medium and supplied to various customers or manufacturing facilities to load into the fabrication machines that make the logic or processor. Some embodiments may be implemented, for example, using a machine-readable medium or article which may store an instruction or a set of instructions that, if executed by a machine, may cause the machine to perform a method and/or operations in accordance with the embodiments. Such a machine may include, for example, any suitable processing platform, computing platform, computing device, processing device, computing system, processing system, computer, processor, or the like, and may be implemented using any suitable combination of

hardware and/or software. The machine-readable medium or article may include, for example, any suitable type of memory unit, memory device, memory article, memory medium, storage device, storage article, storage medium and/or storage unit, for example, memory, removable or non-removable media, erasable or non-erasable media, writeable or re-writeable media, digital or analog media, hard disk, floppy disk, Compact Disk Read Only Memory (CD-ROM), Compact Disk Recordable (CD-R), Compact Disk Rewriteable (CD-RW), optical disk, magnetic media, magneto-optical media, removable memory cards or disks, various types of Digital Versatile Disk (DVD), a tape, a cassette, or the like. The instructions may include any suitable type of code, such as source code, compiled code, interpreted code, executable code, static code, dynamic code, encrypted code, and the like, implemented using any suitable high-level, low-level, object-oriented, visual, compiled and/or interpreted programming language.

[0148] The components and features of the devices described above may be implemented using any combination of discrete circuitry, application specific integrated circuits (ASICs), logic gates and/or single chip architectures. Further, the features of the devices may be implemented using microcontrollers, programmable logic arrays and/or microprocessors or any combination of the foregoing where suitably appropriate. It is noted that hardware, firmware and/or software elements may be collectively or individually referred to herein as “logic” or “circuit.”

[0149] FIG. 10 is a timing diagram illustrating an example sequence for providing authenticated access according to one or more embodiments of the present disclosure. Sequence flow 1000 may include contactless card 102 and computing device 104, which may include an application 1002 and processor 1004. The application 1002 can be any of the applications Printable document 144, 144, Printable document 144, or any other application that executes on the computing device 104.

[0150] At line 1008, the application 1002 communicates with the contactless card 102 (e.g., after being brought near the contactless card 102). Communication between the application 1002 and the contactless card 102 may involve the contactless card 102 being sufficiently close to a card reader (not shown) of the computing device 104 to enable NFC data transfer between the application 1002 and the contactless card 102.

[0151] At line 1006, after communication has been established between computing device 104 and contactless card 102, contactless card 102 generates a message authentication code (MAC) cryptogram. In some examples, this may occur when the contactless card 102 is read by the

application 1002. In particular, this may occur upon a read, such as an NFC read, of a near field data exchange (NDEF) tag, which may be created in accordance with the NFC Data Exchange Format. For example, a reader application, such as application 1002, may transmit a message, such as an applet select message, with the applet ID of an NDEF producing applet. Upon confirmation of the selection, a sequence of select file messages followed by read file messages may be transmitted. For example, the sequence may include “Select Capabilities file,” “Read Capabilities file,” and “Select NDEF file.” At this point, a counter value maintained by the contactless card 102 may be updated or incremented, which may be followed by “Read NDEF file.” At this point, the message may be generated which may include a header and a shared secret. Session keys may then be generated. The MAC cryptogram may be created from the message, which may include the header and the shared secret. The MAC cryptogram may then be concatenated with one or more blocks of random data, and the MAC cryptogram and a random number (RND) may be encrypted with the session key. Thereafter, the cryptogram and the header may be concatenated, and encoded as ASCII hex and returned in NDEF message format (responsive to the “Read NDEF file” message).

[0152] In some examples, the MAC cryptogram may be transmitted as an NDEF tag, and in other examples the MAC cryptogram may be included with a uniform resource indicator (e.g., as a formatted string). In some examples, application 1002 may be configured to transmit a request to contactless card 102, the request comprising an instruction to generate a MAC cryptogram.

[0153] At line 1010, the contactless card 102 sends the MAC cryptogram to the application 1002. In some examples, the transmission of the MAC cryptogram occurs via NFC, however, the present disclosure is not limited thereto. In other examples, this communication may occur via Bluetooth, Wi-Fi, or other means of wireless data communication. At line 1012, the application 1002 communicates the MAC cryptogram to the processor 1004.

[0154] At line 1014, the processor 1004 verifies the MAC cryptogram pursuant to an instruction from the application 122. For example, the MAC cryptogram may be verified, as explained below. In some examples, verifying the MAC cryptogram may be performed by a device other than computing device 104, such as a server of a banking system in data communication with the computing device 104. For example, processor 1004 may output the MAC cryptogram for transmission to the server of the banking system, which may verify the MAC cryptogram. In some examples, the MAC cryptogram may function as a digital signature

for purposes of verification. Other digital signature algorithms, such as public key asymmetric algorithms, e.g., the Digital Signature Algorithm and the RSA algorithm, or zero knowledge protocols, may be used to perform this verification.

[0155] FIG. 11 illustrates a diagram of a system 1100 configured to implement one or more embodiments of the present disclosure. As explained below, during the contactless card creation process, two cryptographic keys may be assigned uniquely for each card. The cryptographic keys may comprise symmetric keys which may be used in both encryption and decryption of data. Triple DES (3DES) algorithm may be used by EMV, and it is implemented by hardware in the contactless card. By using a key diversification process, one or more keys may be derived from a master key based upon uniquely identifiable information for each entity that requires a key.

[0156] Regarding master key management, two issuer master keys 1102, 1126 may be required for each part of the portfolio on which the one or more applets is issued. For example, the first master key 1102 may comprise an Issuer Cryptogram Generation/Authentication Key (Iss-Key-Auth) and the second master key 1126 may comprise an Issuer Data Encryption Key (Iss-Key-DEK). As further explained herein, two issuer master keys 1102, 1126 are diversified into card master keys 1108, 1120, which are unique for each card. In some examples, a network profile record ID (pNPR) 522 and derivation key index (pDKI) 1124, as back-office data, may be used to identify which Issuer Master Keys 1102, 1126 to use in the cryptographic processes for authentication. The system performing the authentication may be configured to retrieve values of pNPR 1122 and pDKI 1124 for a contactless card at the time of authentication.

[0157] In some examples, to increase the security of the solution, a session key may be derived (such as a unique key per session) but rather than using the master key, the unique card-derived keys and the counter may be used as diversification data, as explained above. For example, each time the card is used in operation, a different key may be used for creating the message authentication code (MAC) and for performing the encryption. Regarding session key generation, the keys used to generate the cryptogram and encipher the data in the one or more applets may comprise session keys based on the card unique keys (Card-Key-Auth 1108 and Card-Key-Dek 1120). The session keys (Aut-Session-Key 1130 and DEK-Session-Key 1110) may be generated by the one or more applets and derived by using the application transaction counter (pATC) 1104 with one or more algorithms. To fit data into the one or more algorithms, only the 2 low order bytes of the 4-byte pATC 1104 is used. In some examples, the four byte

session key derivation method may comprise: $F1 := \text{PATC (lower 2 bytes)} \parallel 'F0' \parallel '00' \parallel \text{PATC (four bytes)}$ $F1 := \text{PATC (lower 2 bytes)} \parallel '0F' \parallel '00' \parallel \text{PATC (four bytes)}$ $SK := \{(\text{ALG (MK)} [F1]) \parallel \text{ALG (MK)} [F2]\}$, where ALG may include 3DES ECB and MK may include the card unique derived master key.

[0158] As described herein, one or more MAC session keys may be derived using the lower two bytes of pATC 1104 counter. At each tap of the contactless card, pATC 1104 is configured to be updated, and the card master keys Card-Key-AUTH 508 and Card-Key-DEK 1120 are further diversified into the session keys Aut-Session-Key 1130 and DEK-Session-KEY 1110. pATC 1104 may be initialized to zero at personalization or applet initialization time. In some examples, the pATC 1104 counter may be initialized at or before personalization and may be configured to increment by one at each NDEF read.

[0159] Further, the update for each card may be unique, and assigned either by personalization, or algorithmically assigned by pUID or other identifying information. For example, odd numbered cards may increment or decrement by 2 and even numbered cards may increment or decrement by 5. In some examples, the update may also vary in sequential reads, such that one card may increment in sequence by 1, 3, 5, 2, 2, ... repeating. The specific sequence or algorithmic sequence may be defined at personalization time, or from one or more processes derived from unique identifiers. This can make it harder for a replay attacker to generalize from a small number of card instances.

[0160] The authentication message may be delivered as the content of a text NDEF record in hexadecimal ASCII format. In some examples, only the authentication data and an 8-byte random number followed by MAC of the authentication data may be included. In some examples, the random number may precede cryptogram A and may be one block long. In other examples, there may be no restriction on the length of the random number. In further examples, the total data (i.e., the random number plus the cryptogram) may be a multiple of the block size. In these examples, an additional 8-byte block may be added to match the block produced by the MAC algorithm. As another example, if the algorithms employed used 16-byte blocks, even multiples of that block size may be used, or the output may be automatically, or manually, padded to a multiple of that block size.

[0161] The MAC may be performed by a function key (AUT-Session-Key) 1130. The data specified in cryptogram may be processed with javacard.signature method: `ALG_DES_MAC8_ISO9797_1_M2_ALG3` to correlate to EMV ARQC verification methods.

The key used for this computation may comprise a session key AUT-Session-Key 1130, as explained above. As explained above, the low order two bytes of the counter may be used to diversify for the one or more MAC session keys. As explained below, AUT-Session-Key 1130 may be used to MAC data 1106, and the resulting data or cryptogram An 1114 and random number RND may be encrypted using DEK-Session-Key 1110 to create cryptogram B or output 1118 sent in the message.

[0162] In some examples, one or more HSM commands may be processed for decrypting such that the final 16 (binary, 32 hex) bytes may comprise a 3DES symmetric encrypting using CBC mode with a zero IV of the random number followed by MAC authentication data. The key used for this encryption may comprise a session key DEK-Session-Key 1110 derived from the Card-Key-DEK 1120. In this case, the ATC value for the session key derivation is the least significant byte of the counter pATC 1104.

[0163] The format below represents a binary version example embodiment. Further, in some examples, the first byte may be set to ASCII ‘A.’

Message Format				
1	2	4	8	8
0x43 (Message Type ‘A’)	Version	pATC	RND	Cryptogram A (MAC)
Cryptogram A (MAC)	8 bytes			
MAC of				
2	8	4	4	18 bytes input data
Version	pUID	pATC	Shared Secret	

Message Format			
1	2	4	16
0x43 (Message Type ‘A’)	Version	pATC	Cryptogram B

Cryptogram A (MAC)	8 bytes			
MAC of				
2	8	4	4	18 bytes input data
Version	pUID	pATC	Shared Secret	
Cryptogram B	16			
Sym Encryption of				
8	8			
RND	Cryptogram A			

[0164] Another exemplary format is shown below. In this example, the tag may be encoded in hexadecimal format.

Message Format				
2	8	4	8	8
Version	pUID	pATC	RND	Cryptogram A (MAC)
8 bytes				
8	8	4	4	18 bytes input data
pUID	pUID	pATC	Shared Secret	

Message Format			
2	8	4	16
Version	pUID	pATC	Cryptogram B
8 bytes			

8		4	4	18 bytes input data
pUID	pUID	pATC	Shared Secret	
Cryptogram B	16			
Sym Encryption of				
8	8			
RND	Cryptogram A			

[0165] The UID field of the received message may be extracted to derive, from master keys Iss-Key-AUTH 905 and Iss-Key-DEK 910, the card master keys (Card-Key-Auth 925 and Card-Key-DEK 930) for that particular card. Using the card master keys (Card-Key-Auth 508 and Card-Key-DEK 1120), the counter (pATC) field of the received message may be used to derive the session keys (Aut-Session-Key 1130 and DEK-Session-Key 1110) for that particular card. Cryptogram B 1118 may be decrypted using the DEK-Session-KEY, which yields cryptogram An 1114 and RND, and RND may be discarded. The UID field may be used to look up the shared secret of the contactless card which, along with the Ver, UID, and pATC fields of the message, may be processed through the cryptographic MAC using the re-created Aut-Session-Key to create a MAC output, such as MAC'. If MAC' is the same as cryptogram An 1114, then this indicates that the message decryption and MAC checking have all passed. Then the pATC may be read to determine if it is valid.

[0166] During an authentication session, one or more cryptograms may be generated by the one or more applications. For example, the one or more cryptograms may be generated as a 3DES MAC using ISO 9797-1 Algorithm 3 with Method 2 padding via one or more session keys, such as Aut-Session-Key 1130. The input data 1106 may take the following form: Version (2), pUID (8), pATC (4), Shared Secret (4). In some examples, the numbers in the brackets may comprise length in bytes. In some examples, the shared secret may be generated by one or more random number generators which may be configured to ensure, through one or more secure processes, that the random number is unpredictable. In some examples, the shared secret may comprise a random 4-byte binary number injected into the card at personalization

time that is known by the authentication service. During an authentication session, the shared secret may not be provided from the one or more applets to the mobile application. Method 2 padding may include adding a mandatory 0x'80' byte to the end of input data and 0x'00' bytes that may be added to the end of the resulting data up to the 8-byte boundary. The resulting cryptogram may comprise 8 bytes in length.

[0167] In some examples, one benefit of encrypting an unshared random number as the first block with the MAC cryptogram, is that it acts as an initialization vector while using CBC (Block chaining) mode of the symmetric encryption algorithm. This allows the “scrambling” from block to block without having to pre-establish either a fixed or dynamic IV.

[0168] By including the application transaction counter (pATC) as part of the data included in the MAC cryptogram, the authentication service may be configured to determine if the value conveyed in the clear data has been tampered with. Moreover, by including the version in the one or more cryptograms, it is difficult for an attacker to purposefully misrepresent the application version in an attempt to downgrade the strength of the cryptographic solution. In some examples, the pATC may start at zero and be updated by 1 each time the one or more applications generates authentication data. The authentication service may be configured to track the pATCs used during authentication sessions. In some examples, when the authentication data uses a pATC equal to or lower than the previous value received by the authentication service, this may be interpreted as an attempt to replay an old message, and the authenticated may be rejected. In some examples, where the pATC is greater than the previous value received, this may be evaluated to determine if it is within an acceptable range or threshold, and if it exceeds or is outside the range or threshold, verification may be deemed to have failed or be unreliable. In the MAC operation 1112, data 1106 is processed through the MAC using Aut-Session-Key 1130 to produce MAC output (cryptogram A) 1114, which is encrypted.

[0169] In order to provide additional protection against brute force attacks exposing the keys on the card, it is desirable that the MAC cryptogram 1114 be enciphered. In some examples, data or cryptogram An 1114 to be included in the ciphertext may comprise: Random number (8), cryptogram (8). In some examples, the numbers in the brackets may comprise length in bytes. In some examples, the random number may be generated by one or more random number generators which may be configured to ensure, through one or more secure processes, that the random number is unpredictable. The key used to encipher this data may comprise a session

key. For example, the session key may comprise DEK-Session-Key 1110. In the encryption operation 1116, data or cryptogram A 1114 and RND are processed using DEK-Session-Key 510 to produce encrypted data, cryptogram B 1118. The data 1114 may be enciphered using 3DES in cipher block chaining mode to ensure that an attacker must run any attacks over all of the ciphertext. As a non-limiting example, other algorithms, such as Advanced Encryption Standard (AES), may be used. In some examples, an initialization vector of 0x'0000000000000000' may be used. Any attacker seeking to brute force the key used for enciphering this data will be unable to determine when the correct key has been used, as correctly decrypted data will be indistinguishable from incorrectly decrypted data due to its random appearance.

[0170] In order for the authentication service to validate the one or more cryptograms provided by the one or more applets, the following data must be conveyed from the one or more applets to the mobile device in the clear during an authentication session: version number to determine the cryptographic approach used and message format for validation of the cryptogram, which enables the approach to change in the future; pUID to retrieve cryptographic assets, and derive the card keys; and pATC to derive the session key used for the cryptogram.

[0171] FIG. 12 illustrates a method 1200 for generating a cryptogram. For example, at block 1202, a network profile record ID (pNPR) and derivation key index (pDKI) may be used to identify which Issuer Master Keys to use in the cryptographic processes for authentication. In some examples, the method may include performing the authentication to retrieve values of pNPR and pDKI for a contactless card at the time of authentication.

[0172] At block 1204, Issuer Master Keys may be diversified by combining them with the card's unique ID number (pUID) and the PAN sequence number (PSN) of one or more applets, for example, a payment applet.

[0173] At block 1206, Card-Key-Auth and Card-Key-DEK (unique card keys) may be created by diversifying the Issuer Master Keys to generate session keys which may be used to generate a MAC cryptogram.

[0174] At block 1208, the keys used to generate the cryptogram and encipher the data in the one or more applets may comprise the session keys of block 1030 based on the card unique keys (Card-Key-Auth and Card-Key-DEK). In some examples, these session keys may be generated by the one or more applets and derived by using pATC, resulting in session keys Aut-Session-Key and DEK-Session-Key.

[0175] FIG. 13 depicts an exemplary process 1300 illustrating key diversification according to one example. Initially, a sender and the recipient may be provisioned with two different master keys. For example, a first master key may comprise the data encryption master key, and a second master key may comprise the data integrity master key. The sender has a counter value, which may be updated at block 1302, and other data, such as data to be protected, which it may secure share with the recipient.

[0176] At block 1304, the counter value may be encrypted by the sender using the data encryption master key to produce the data encryption derived session key, and the counter value may also be encrypted by the sender using the data integrity master key to produce the data integrity derived session key. In some examples, a whole counter value or a portion of the counter value may be used during both encryptions.

[0177] In some examples, the counter value may not be encrypted. In these examples, the counter may be transmitted between the sender and the recipient in the clear, i.e., without encryption.

[0178] At block 1306, the data to be protected is processed with a cryptographic MAC operation by the sender using the data integrity session key and a cryptographic MAC algorithm. The protected data, including plaintext and shared secret, may be used to produce a MAC using one of the session keys (AUT-Session-Key).

[0179] At block 1308, the data to be protected may be encrypted by the sender using the data encryption derived session key in conjunction with a symmetric encryption algorithm. In some examples, the MAC is combined with an equal amount of random data, for example each 8 bytes long, and then encrypted using the second session key (DEK-Session-Key).

[0180] At block 1310, the encrypted MAC is transmitted, from the sender to the recipient, with sufficient information to identify additional secret information (such as shared secret, master keys, etc.), for verification of the cryptogram.

[0181] At block 1312, the recipient uses the received counter value to independently derive the two derived session keys from the two master keys as explained above.

[0182] At block 1314, the data encryption derived session key is used in conjunction with the symmetric decryption operation to decrypt the protected data. Additional processing on the exchanged data will then occur. In some examples, after the MAC is extracted, it is desirable to reproduce and match the MAC. For example, when verifying the cryptogram, it may be decrypted using appropriately generated session keys. The protected data may be reconstructed

for verification. A MAC operation may be performed using an appropriately generated session key to determine if it matches the decrypted MAC. As the MAC operation is an irreversible process, the only way to verify is to attempt to recreate it from source data.

[0183] At block 1316, the data integrity derived session key is used in conjunction with the cryptographic MAC operation to verify that the protected data has not been modified.

[0184] Some examples of the methods described herein may advantageously confirm when a successful authentication is determined when the following conditions are met. First, the ability to verify the MAC shows that the derived session key was proper. The MAC may only be correct if the decryption was successful and yielded the proper MAC value. The successful decryption may show that the correctly derived encryption key was used to decrypt the encrypted MAC. Since the derived session keys are created using the master keys known only to the sender (e.g., the transmitting device) and recipient (e.g., the receiving device), it may be trusted that the contactless card which originally created the MAC and encrypted the MAC is indeed authentic. Moreover, the counter value used to derive the first and second session keys may be shown to be valid and may be used to perform authentication operations.

[0185] Thereafter, the two derived session keys may be discarded, and the next iteration of data exchange will update the counter value (returning to block 1302) and a new set of session keys may be created (at block 1310). In some examples, the combined random data may be discarded.

[0186] It will be appreciated that the exemplary devices shown in the block diagrams described above may represent one functionally descriptive example of many potential implementations. Accordingly, division, omission or inclusion of block functions depicted in the accompanying figures does not infer that the hardware components, circuits, software and/or elements for implementing these functions would necessarily be divided, omitted, or included in embodiments.

[0187] At least one computer-readable storage medium may include instructions that, when executed, cause a system to perform any of the computer-implemented methods described herein.

[0188] Some embodiments may be described using the expression “one embodiment” or “an embodiment” along with their derivatives. These terms mean that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment. The appearances of the phrase “in one embodiment” in various places in the

specification are not necessarily all referring to the same embodiment. Moreover, unless otherwise noted the features described above are recognized to be usable together in any combination. Thus, any features discussed separately may be employed in combination with each other unless it is noted that the features are incompatible with each other.

[0189] It is emphasized that the Abstract of the Disclosure is provided to allow a reader to quickly ascertain the nature of the technical disclosure. It is submitted with the understanding that it will not be used to interpret or limit the scope or meaning of the claims. In addition, in the foregoing Detailed Description, it can be seen that various features are grouped together in a single embodiment for the purpose of streamlining the disclosure. This method of disclosure is not to be interpreted as reflecting an intention that the claimed embodiments require more features than are expressly recited in each claim. Rather, as the following claims reflect, inventive subject matter lies in less than all features of a single disclosed embodiment. Thus, the following claims are hereby incorporated into the Detailed Description, with each claim standing on its own as a separate embodiment. In the appended claims, the terms "including" and "in which" are used as the plain-English equivalents of the respective terms "comprising" and "wherein," respectively. Moreover, the terms "first," "second," "third," and so forth, are used merely as labels, and are not intended to impose numerical requirements on their objects.

[0190] What has been described above includes examples of the disclosed architecture. It is, of course, not possible to describe every conceivable combination of components and/or methodologies, but one of ordinary skill in the art may recognize that many further combinations and permutations are possible. Accordingly, the novel architecture is intended to embrace all such alterations, modifications and variations that fall within the spirit and scope of the appended claims.

[0191] The foregoing description of example embodiments has been presented for the purposes of illustration and description. It is not intended to be exhaustive or to limit the present disclosure to the precise forms disclosed. Many modifications and variations are possible in light of this disclosure. It is intended that the scope of the present disclosure be limited not by this detailed description, but rather by the claims appended hereto. Future filed applications claiming priority to this application may claim the disclosed subject matter in a different manner and may generally include any set of one or more limitations as variously disclosed or otherwise demonstrated herein.

CLAIMS

What is claimed is:

1. A computer-implemented method to enable self-service printing with authentication, the computer-implemented method including:
 - receiving, by a server, a print-request to print a document associated with an account, the print-request received from a computing device;
 - adding, by the server, a print job for the document in a print queue associated with the account;
 - receiving, by the server, a second request to initiate printing the document associated with the account, the second request received from a printer;
 - and
 - releasing, by the server, the print queue associated with the account to cause the printer to print the document, the releasing being responsive to the second request being authenticated.
2. The computer-implemented method of claim 1, wherein authenticating the print-request by the computing device includes a first authentication routine and authenticating the second request by the printer includes a second authentication routine.
3. The computer-implemented method of claim 2, wherein the first authentication routine is based on a setting stored in the computing device.
4. The computer-implemented method of claim 2, wherein the first authentication routine is based on a contactless card.
5. The computer-implemented method of claim 4, wherein the second authentication routine is based on the contactless card and the computing device.
6. The computer-implemented method of claim 2, wherein the second authentication routine is based on a contactless card.
7. The computer-implemented method of claim 1, further including, in response to receiving the print-request to print the document, suggesting, by the server, one or more printers to print the document.

8. The computer-implemented method of claim 7, wherein the one or more printers are suggested based on a type of the document.
9. The computer-implemented method of claim 1, wherein releasing the print queue includes verifying, by the server, that the printer is authorized to print the document based on a type of the document.
10. A computer-implemented method to enable self-service printing with authentication, the computer-implemented method including:
- selecting, by a computing device, for printing, a document associated with an account;
 - generating, by the computing device, a list of printers for printing the document, the list is generated based on a type of the document;
 - selecting, by the computing device, from the list, a printer to print the document; and
 - providing, by the computing device, in response to the printer being accessed to print the document, an authentication code that causes the printer to print the document.
11. The computer-implemented method of claim 10, wherein the list is generated further based on a location of the computing device.
12. The computer-implemented method of claim 10, wherein the document is a plurality of documents, and the list of printers is generated based on the type of a first document from the plurality of documents.
13. The computer-implemented method of claim 10, wherein the type of the document is at least one of a report, an account statement, a transaction history, a check, a money transfer instruction, a form, a letter, an offer, and a combination thereof.
14. The computer-implemented method of claim 10, wherein, the authentication code is provided as a machine-readable code to be scanned by the printer.
15. The computer-implemented method of claim 10, wherein the authentication code is received by the computing device from a server in response to a contactless card-based authentication by the computing device.
16. A computing apparatus including:
- a processor; and

a memory storing instructions that, when executed by the processor, configure the computing apparatus to:

receive a first request to print a document associated with an account, the first request received from a computing device;

add a print job for the document in a print queue associated with the account;

receive a second request to initiate printing the document associated with the document, the second request received from a printer; and

release the print queue associated with the account to cause the printer to print the document, the release being responsive to the second request being authenticated.

17. The computing apparatus of claim 16, wherein the computing device authenticates the first request using a first authentication routine, and the printer authenticates the second request using a second authentication routine.

18. The computing apparatus of claim 16, wherein the second request is authenticated using a contactless card and the computing device.

19. The computing apparatus of claim 16, wherein the second request is authenticated using a contactless card and the printer.

20. The computing apparatus of claim 16, wherein the print queue is released in response to verification that the printer is authorized to print the document.