

AUTHENTICATED MESSAGING SESSION WITH CONTACTLESS CARD**AUTHENTICATION****Cross-Reference to Related Applications**

[0001] This application claims priority to U.S. Patent Application Serial No. 17/231,481, entitled “AUTHENTICATED MESSAGING SESSION WITH CONTACTLESS CARD AUTHENTICATION” filed on April 15, 2021. The contents of the aforementioned patent application are incorporated herein by reference in their/its entirety.

Background

[0002] Financial institutions, like banks and brokerage houses, have begun to employ programmatic intelligent agents, like chatbots, to interact with customers online. The programmatic intelligent agents may be deployed in a number of digital channels, including with messaging services, such as Short Message Service (SMS) (“text”). One challenge with the SMS digital channel is that it is relatively insecure. There is no guarantee that a party communicating via SMS is who they present themselves as. Moreover, unwanted observers may observe SMS messaging sessions. Thus, when a customer texts a programmatic intelligent agent of a financial institution for confidential information, such as the routing number for the checking account of the customer, it is problematic for the programmatic intelligent agent to provide the confidential information to the customer via an SMS message.

Summary

[0003] In accordance with a first inventive aspect, a method includes receiving a message from a party via a messaging service at a programmatic intelligent agent running on a processor of a computing device. The message requests a response message from the programmatic intelligent agent. The processor determines that authentication by contactless card is needed. A request message is sent from the programmatic intelligent agent to the party. The request message contains information for launching code for authenticating the party via contactless card. Confirmation is received at the programmatic intelligent agent that the party has been authenticated via contactless card. An authenticated messaging session is initiated between the party and the programmatic intelligent agent.

[0004] The received message from the party may request access to confidential information or sensitive information. The method may include generating and sending the response message to the party. The response message may contain at least some of the confidential information or at least some of the sensitive information. The party may have a secure account with an institution, and the method may include the programmatic intelligent agent accessing the secure account to generate the response message. The received message

from the party may request a financial transaction. The messaging service may be a Short Message Service (SMS) messaging service. A time limit to the authenticated messaging session may be established such that, at expiration of the time limit, the messaging session is no longer authenticated

[0005] In accordance with another inventive aspect, a method includes initiating the sending of a message via a messaging service with a processor of a device, where the message seeks a response message to a programmatic intelligent agent. In response to the sending of the message, a prompt from the programmatic intelligent agent is received via the messaging service to authenticate identity via a contactless card. Information from the contactless card is obtained by the processor. The processor forwards the obtained information to an authenticating authority to authenticate the identity. Where the authentication by the authenticating authority is successful, the response message is received from the programmatic intelligent agent.

[0006] The obtaining of the information from the contactless card may be responsive to the contactless card being in proximity with the device. The device may include Near Field Communication (NFC) capabilities, and the information may be obtained by NFC with the contactless card. The obtained information may include credentials and identity information. The information may be obtained and forwarded in encrypted and/or hashed form. A request message may be received via the messaging service from the programmatic intelligent agent. The request message may have a link to launch an application on the device for authenticating the identity. The message seeking the response message may request information regarding a secure account at a financial institution. The message seeking the response message may request a financial transaction. The device may be a smartphone, and the prompt may contain a link to launch an application installed on the smartphone to authenticate identity via the contactless card.

[0007] In accordance with a further inventive aspect, a non-transitory computer-readable storage medium stores computer programming instructions. When the computer programming instructions are executed by a processor cause the processor to receive confirmation at a programmatic intelligent agent that an identity of a party has been confirmed by a contactless card interaction. The instructions also cause the processor to establish an authenticated messaging session for the with the programmatic intelligent agent with the party. Stored information regarding a secure account of the party is processed to glean an insight regarding the secure account. A message is sent from the programmatic intelligent agent to the party as part of the authenticated messaging session. The message contains information regarding the insight gleaned from processing the stored information regarding the secure account of the party.

[0008] The insight may be that there likely has been fraudulent activity with the account. The insight may be that activity in the account differs from historical activity in the secure account. The insight may be that the party could benefit from a service given the information regarding the secure account.

Brief Description of the Drawings

[0009] Figure 1 depicts a block diagram of an illustrative messaging system suitable for exemplary embodiments.

[0010] Figure 2 depicts a diagram illustrating different type of devices a user may use to participate in an authenticated messaging session in exemplary embodiments.

[0011] Figure 3A depicts actions that may be taken for a successful authentication of the user per exemplary embodiments.

[0012] Figure 3B depicts actions that may be taken for an unsuccessful authentication of a user per exemplary embodiments.

[0013] Figure 4A depicts a flowchart of steps that may be performed in exemplary embodiments in authenticating the identity of the user.

[0014] Figure 4B depicts a block diagram of components that may be part of the authentication of the user on the user side of the messaging system in exemplary embodiments.

[0015] Figures 5A and 5B depicts an illustrative contactless card that may be used in exemplary embodiments.

[0016] Figure 6A depicts inputs and outputs of a hash function that may be used to create a hash value for securing information for a secure package in exemplary embodiments.

[0017] Figure 6B depicts different types of inputs that may be fed into the hash function in exemplary embodiments.

[0018] Figure 7 depicts the creation of a secure package in exemplary embodiments.

[0019] Figure 8 depicts certain information stored and used by the authentication service in exemplary embodiments.

[0020] Figure 9 depicts a flowchart of illustrative steps that may be performed in authenticating the identity of the user in exemplary embodiments.

[0021] Figure 10 depicts example of other factors that may be examined in authenticating the identity of the user in exemplary embodiments.

[0022] Figure 11 depicts an illustrative exchange of messages in an exemplary embodiment.

[0023] Figure 12 depicts a flowchart of illustrative steps that may be performed in relation to expiration of an authenticated messaging session in exemplary embodiments.

[0024] Figure 13 depicts a flowchart of steps that may be performed in identifying and outputting insights gleaned by processing data regarding a user or a user account in exemplary embodiments.

[0025] Figure 14A, 14B and 14C depicts example of messages that may be output to share insights gained by processing data regarding the user or user account in exemplary embodiments.

Detailed Description

[0026] The exemplary embodiments described herein overcome the above-described problems with conventional systems by providing an authenticated messaging environment in which a user can securely message with a programmatic intelligent agent. The user may be authenticated at the prompting of the programmatic intelligent agent, such as the beginning of a messaging session or when the user submits a request that requires access to sensitive or confidential information or requires access to a secure account. The prompt may take the form of a message sent from the programmatic intelligent agent. The message may contain a link for launching code, such as an application, that facilitates authentication of the user's identity. The user may activate the link to launch the code and then perform the steps requested by the code to perform the authentication. By providing the link as part of the messaging session, the programmatic intelligent agent initiates the authentication in the messaging environment. There is no need for the user to exit the messaging application and launch a separate application.

[0027] In the exemplary embodiments, the authentication may entail the user using a contactless card. The contactless card may contain information regarding the user and may generate a secure package containing credentials of the user and other information regarding the user. The contactless card may support Near Field Communication (NFC) wireless communications. The user has a device, such as a smartphone with messaging capabilities. The device may have NFC capabilities, and the user may be required to tap the contactless card with an NFC reader in the device to cause information to be extracted from the contactless card, such as credentials and other information for the secure package. The secure package may be sent via a connection, such as a wireless phone connection, to an authentication service. The authentication service receives the secure package, extracts the credentials and information regarding the user from the secure package and attempts to authenticate the identity of the user based at least in part on the extracted information. The result of the authentication may be communicated from the authentication service to the programmatic intelligent agent. If the result is that the identity of the user is authenticated, the programmatic intelligent agent may begin an authenticated messaging session with the user. If result is that the identity of the user is

not authenticated, the programmatic intelligent agent may indicate that the authentication has failed and refuse to initiate an authenticated messaging session.

[0028] The authenticated messaging session may have an associated expiration time. Once the expiration time is reached, the authenticated messaging session ends. The programmatic intelligent agent may prompt the user to reauthenticate. This expiration provides an added degree of security to ensure that an imposter has not taken over the session. Moreover, the expiration time ensures that the session does not continue indefinitely with little activity. Such an extended messaging session poses a security risk.

[0029] The programmatic intelligent agent may process data associated with the user and/or an account of the user. The processing of the data may yield insights that may be shared with the user. For example, the programmatic intelligent agent may process the data to identify that there is suspicious activity in an account of the user, such as a large withdrawal, and generate a message as part of the authenticated messaging session flagging the suspicious activity to the user. As another example, the processing of the data may yield that the user is spending more than usual that month. The programmatic intelligent agent may generate a message as part of the authenticated messaging session noting this unusual activity. As a final example, the processing may indicate that the user may be a candidate for refinancing of their mortgage. The programmatic intelligent agent may send a message to the user as part of the authenticated messaging session indicating that the user may save money by refinancing and may present refinancing options.

[0030] Figure 1 depicts a block diagram of a messaging environment 100 suitable for exemplary embodiments. The messaging environment 100 includes a computing device 102 that a user 118 uses to communicate with a programmatic intelligent agent 128 via a messaging service. The computing device 102 may be any of a number of different types of devices that support such messaging via the messaging service. Figure 2 depicts a diagram 200 of different device types 202 that may be used by a user 118 in the exemplary embodiments. For instance, the computing device 102 may be a smartphone 204 or a smartwatch 212 with messaging capability. The computing device may be a tablet computer 206 with messaging capability. The computing device 102 may be a laptop computer 208 or a desktop computer with messaging capability. The computing device 102 may also be another type of computing device 214. The computing device 102 should have a messaging capability and should support interaction with a contactless card 120, such as through NFC. The contactless card 120 may store a synchronized counter 115 that may be used in encryption as will be explained below.

[0031] The computing device 102 may include one or more processors 108. Each processor 108 may execute instructions to perform functionality described herein. Each processor 108 may be a Central Processing Unit (CPU), a Graphics Processing Unit (GPU), an Application Specific Integrated Circuit (ASIC), a Field Programmable Gate Array (FPGA) or a controller with processing capabilities.

[0032] The computing device 102 may include a storage 110. The storage 110 may include one or more memory and storage devices, including but not limited to both primary and secondary storage devices, such as Random Access Memory (RAM) devices, Read Only Memory (ROM) devices, solid state memory devices, flash memory devices, registers, magnetic memory devices, optical memory devices and other types of non-transitory computer readable storage media. The storage 110 may hold computer programming instructions for a messaging application, such as a SMS messaging application, an instant messaging application, a social media messaging application, a chat application or other variety of messaging service. The storage 110 may hold an application 114. The application 114 enables a user to gain access to a web server for a given entity, such as a merchant, financial institution, brokerage house, or other variety of institution. The application 114 is the code that is launched to facilitate authentication of the identity of the user 118. For example, the application 114 may be an application for a financial institution that enables a user to perform financial transactions and access information regarding an account of the user 118.

[0033] The computing device 102 also may include an integrated circuit (IC) that provides NFC capabilities 116. This may be any of a number NFC IC's that are commercially available, such as those found in NFC-compatible phones. The NFC IC 116 has an NFC reader which is able to read a contactless card 120 of the user 118. The NFC IC 116 also includes a coil antenna. As will be described below, the contactless card 120 may hold credentials for the user 118 and user information that may be communicated via a contactless wireless protocol like NFC.

[0034] The messaging environment 100 also includes a server 104. The computing device 102 may communicate with the server 104 via one or more networks 106. The network(s) 106 may include the Internet, one or more Local Area Networks (LANs), cellular phone networks and/or wireless networks, such as WiFi (IEEE 802.11) networks. The server 104 is a computing device that includes processor(s) 122 for executing computer programming instructions. The processor(s) may take the form of processor described above relative processor(s) 108. The server 104 may provide cloud services that are accessible to the user 118 via the computing device 102.

[0035] The server 104 includes storage 124. The storage 124 may include a number of different storage devices and/or memory devices of the types, such as described above regarding storage 110. The storage 124 may store a messaging application 126 and a programmatic intelligent agent 128 that may be executed by the processor(s) 122 to provide the functionality described herein. The messaging application 126 enables the programmatic intelligent agent 128 to participate in a messaging service, such as an SMS or other type of messaging service as detailed above. The programmatic intelligent agent 128 is an agent implemented with computer programming instructions that may perform intelligent tasks as described herein. The programmatic intelligent agent 128 possesses a natural language capability to generate textual messages and to respond to textual messages appropriately. The programmatic intelligent agent 128 is designed to seem human-like in its interactions. The programmatic intelligent agent 128 parses received messages, extracts meaning from the received messages and generates appropriate responses. The programmatic intelligent agent 128 may be realized as a chatbot. As will be described below, the programmatic intelligent agent 128 may process data 134 stored in a database or elsewhere concerning the user 118 and/or user accounts. The programmatic intelligent agent 128 may initiate transactions, such as in user accounts and has clearance to access confidential and sensitive information regarding the user and/or user account. The processing may yield insights and other information that may guide messaging service interactions with the user 118.

[0036] An authentication service 132 may be provided on another server 130 that is accessible by the user 118 via the network(s) 106. In some embodiments, the authentication service 132 may be resident on server 104 rather than a separate server 130. The authentication service 132 is responsible for authenticating the identity of a party, like the user 118, so that an authenticated messaging session between the user 118 and the programmatic intelligent agent 128 may be conducted. The server 130 may include one or more processors 133 on which the authentication service 132 runs.

[0037] When the user 118 wishes to initiate a messaging session with the programmatic intelligent agent 128, the user uses the messaging application 112 to send a message via the messaging service to the programmatic intelligent agent 128 as shown by 302 in Figure 3A. The sent message requests a response from the programmatic intelligent agent 128. Suppose, for example, that user 118 wishes to know the routing number for a financial institution where the user has an account. The user 118 might send a message with a simple question like “What is my routing number?”. The programmatic intelligent agent 128 may process the message to determine if the message requests access to confidential or sensitive information or access to a

secure account and if the message does, may determine that the identity of the user needs to be authenticated. In other cases, this step of determining that authentication is needed is not performed. Instead, the first message of a session prompts a request for authentication. The programmatic intelligent agent 128 sends a request message back to the user 118 requesting that the user authenticate using the contactless card 120 as shown by 304. The request message contains a link to launch code on the computing device 102 that may be used for the user to authenticate using the contactless card 120. The code may be the application 114. For the example set forth above, the application may be for a financial institution.

[0038] The user 118 receives the link in the request message and activates the application 114 as indicated by 306. This approach makes it easy for the user 118 to authenticate while in the messaging session. There is no need to exit the messaging session and manually log into the application 114. The launched application 114 prompts the user 118 to touch the contactless card 120 to the NFC reader in the NFC IC 116 on the computing device.

[0039] Figure 4A shows a flowchart of the steps that may be performed in an exemplary embodiment to authenticate an initiating party that wishes to initiate a secure messaging service session with a non-initiating party. The steps are described below relative to Figure 4B. The process may begin with a user tapping a contactless card 432 (see Figure 4A) to an NFC reader 428 in the computing device 436 (see 402). The tapping initiates an NFC communication session between the contactless card 432 and the NFC reader 428 in the computing device 436. In other instances, the contactless card 432 need not tap the NFC reader 428 but rather may need only be in sufficient proximity to the NFC reader 428 to initiate an NFC communication session. In the NFC communication session, a secure package 434 is sent from the contactless card 432 to computing device 436. Application 114 is running on the computing device 436 and receives the secure package 434. The application 114 generates a message 440 to the authentication service 132 encapsulating the secure package 442. The message 440 serves as a request to initiate an authenticated messaging system, and the message 440 is sent to the authentication service 132 (see 404 in Figure 4A).

[0040] The authentication service 132 extracts information from the secure package and uses the package to authenticate the identity of the user as indicated by 408 in Figure 4A and by 310 in Figure 3A. The details of the secure package 434 and the contactless card 432 will be discussed below.

[0041] Where the authentication is successful, as shown in Figure 3A, the authentication service 132 informs the programmatic intelligent agent 128 that the authentication was successful as indicated by 312. The programmatic intelligent agent 128 may then create an

authenticated messaging session and send a response message back to the user 118. For instance, the programmatic intelligent agent 128 may advise the user 118 that the authentication was successful and provide the requested response.

[0042] Figure 3B shows the steps that may be performed when the authentication is unsuccessful. The steps 302, 304, 306, 308 and 310 are the same as in Figure 3A. However, the authentication in 310 is unsuccessful. Thus, the authentication service 132 informs the programmatic intelligent agent 128 that the authentication failed as indicated by 316. The programmatic intelligent agent 128 does not create an authenticated messaging session and does not send the requested response to the initial message from the user 118. Instead, the programmatic intelligent agent 128 send a failure message to the user 118 as indicated by 318.

[0043] Figure 5A illustrates an example of a contactless card 500, which may be a payment card, such as a credit card, a debit card, or a gift card, issued by a service provider 505, such as a merchant, financial institution, etc., displayed on the front or back of the card 500. In some exemplary embodiments, the contactless card 500 is not related to a payment card, and may comprise, without limitation, an identification card. In some instances, the payment card may comprise a dual interface contactless payment card. The contactless card 500 may comprise a substrate 510, which may include a single layer or 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 500 may have physical characteristics compliant with the ID-1 format of the ISO/IEC 7810 standard, and the contactless card 500 may otherwise be compliant with the ISO/IEC 14443 standard. However, it is understood that the contactless card 500 according to the present disclosure may have different characteristics, and the present disclosure does not require a contactless card to be implemented in a payment card.

[0044] The contactless card 500 may also include identification information 515 displayed on the front and/or back of the card, and a contact pad 520. The contact pad 520 may be configured to establish contact with another communication device, such as a user device, smart phone, laptop, desktop, or tablet computer. The contactless card 500 may also include processing circuitry, antenna and other components not shown in Figure 5A. These components may be located behind the contact pad 520 or elsewhere on the substrate 510. The contactless card 500 may also include a magnetic strip or tape, which may be located on the back of the card (not shown in Figure 5A).

[0045] As illustrated in Figure 5B, the contact pad 520 of Figure 5A may include processing circuitry 525 for storing and processing information, including a microprocessor 530 and a memory 535. It is understood that the processing circuitry 525 may contain additional components, including processors, memories, error and parity/CRC checkers, data encoders, anti-collision algorithms, controllers, command decoders, security primitives and tamper proofing hardware, as necessary to perform the functions described herein.

[0046] The memory 535 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 500 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. It may also be read many times.

[0047] The memory 535 may be configured to store one or more applets 540, one or more counters 545, and a customer identifier 550. The one or more applets 540 may comprise one or more software applications configured to execute on one or more contactless cards, such as Java Card applet. However, it is understood that applets 540 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 545 may comprise a numeric counter sufficient to store an integer. The customer identifier 550 may comprise a unique alphanumeric identifier assigned to a user of the contactless card 500, and the identifier may distinguish the user of the contactless card from other contactless card users. In some examples, the customer identifier 550 may identify both a customer and an account assigned to that customer and may further identify the contactless card associated with the customer's account.

[0048] The processor 530 and memory 535 elements of the foregoing exemplary embodiments are described with reference to the contact pad, but the present disclosure is not limited thereto. It is understood that these elements may be implemented outside of the pad 520 or entirely separate from it, or as further elements in addition to processor 530 and memory 535 elements located within the contact pad 520.

[0049] In some examples, the contactless card 500 may comprise one or more antennas 555. The one or more antennas 555 may be placed within the contactless card 500 and around the processing circuitry 525 of the contact pad 520. For example, the one or more antennas 555 may be integral with the processing circuitry 525 and the one or more antennas 555 may be used

with an external booster coil. As another example, the one or more antennas 555 may be external to the contact pad 520 and the processing circuitry 525.

[0050] In an embodiment, the coil of contactless card 500 may act as the secondary of an air core transformer. The terminal may communicate with the contactless card 500 by cutting power or amplitude modulation. The contactless card 500 may infer the data transmitted from the terminal using the gaps in the contactless card's power connection, which may be functionally maintained through one or more capacitors. The contactless card 500 may communicate back by switching a load on the contactless card's coil or load modulation. Load modulation may be detected in the terminal's coil through interference.

[0051] As explained above, the contactless card 500 may be built on a software platform operable on smart cards or other devices having limited memory, such as JavaCard, and one or more applications or applets may be securely executed. Applets may be added to contactless cards to provide a one-time password (OTP) for multifactor authentication (MFA) in various mobile application-based use cases. Applets 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, and produce an NDEF message that comprises a cryptographically secure OTP encoded as an NDEF text tag.

[0052] The generation of the secure package 434 (Figure 4B) may employ cryptographic hash functions, such as MD5 or SHA-1. Figure 6A shows a block diagram 600 depicting how the cryptographic hash functions may be used in exemplary embodiments. In the example shown in Figure 6A, three inputs 602, 604 and 606 are passed through a hash function 608 together. The choice of depicting three inputs is intended to be illustrative and not limiting. Other number of inputs may be used in some instances. The hash function 608 produces an output hash value 610. Due to the nature of the hash function 608, it is computationally difficult to derive the inputs 602, 604 and 606 from the hash value 610 without knowing the key 607 used by the hash function 608. The key 607 is kept secret. The key 607 may be dynamically generated for each session and may be particular to the contactless card. Thus, the hash function 608 provides a layer of security for the content (e.g., inputs 602, 604 and 606) that is included in the secure package 404.

[0053] In the exemplary embodiments, the inputs 602, 604 and 606 may vary depending on the information the parties wish to exchange and the protocol for authenticating the initiating party. Figure 6B, shows a diagram 640 of possible types of inputs 642 that may be hashed in exemplary embodiments. In these exemplary embodiments, a onetime password 644 generated by the contactless card may be included as an input. An account identifier 646 for the initiating

party may be provided. This may be an account number or other identifier that uniquely identifies the account of the initiating party. The account identifier 646 may be a phone number for the initiating party. In some cases, the phone number of the initiating party may not be included in the hash value 610 but may be derived from the message sent from the computing device 102. The inputs 642 may include a counter value and/or a name 650 of the initiating party.

[0054] As an added layer of security, the hash value 610 may be encrypted. Figure 7 shows a block diagram 700 depicting such encryption. The hash value 702 generated as discussed above is passed to an encryption engine 704 that encrypts the hash value using an encryption key 706. The resulting output is the secure package 708. The encryption engine 704 may use any of a number of cryptographic algorithms, such as DES, AES, RSA, DSA or the like. These may be symmetric cryptographic algorithms like DES and AES or asymmetric cryptographic algorithms like RSA and DSA. It is presumed that the authentication service 132 possesses the appropriate key to decrypt the secure package. Although not shown in Figure 7, other content may be encrypted in conjunction with the hash value 702.

[0055] Figure 8 depicts certain items stored as part of the authentication service 132. These items include a synchronized counter 802 that may be used in decryption/encryption operations. The authentication service includes decryption code for performing decryption operations on the secure package 434. The authentication service 132 may also store a number of decryption keys and encryption keys 806.

[0056] Generally, the server 130 (or another computing device) and the contactless card 432 may be provisioned with the same master key (also referred to as a master symmetric key). More specifically, each contactless card 432 may be programmed with a distinct master key that has a corresponding pair in the authentication service 132. For example, when a contactless card 432 is manufactured, a unique master key may be programmed into the memory 535 of the contactless card 432. Similarly, the unique master key may be stored in a record of a customer associated with the contactless card 432 in the account information accessible by the authentication service 132 (and/or stored in a different secure location). The master key may be kept secret from all parties other than the contactless card 500 and authentication service 132, thereby enhancing security of the system.

[0057] The master keys may be used in conjunction with the counters to enhance security using key diversification. The counters 115 and 802 comprise values that are synchronized between the contactless card 120 and the authentication service 132. The counter value may

comprise a number that changes each time data is exchanged between the contactless card 120 and the authentication service 132.

[0058] After communication has been established between computing device 102 and the contactless card 120, the contactless card 120 may generate a message authentication code (MAC) cryptogram. In some examples, this may occur when the contactless card 120 is read. 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, such as the NFC reader, 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, the counter value 115 maintained by the contactless card 120 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). 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). The contactless card 120 may then transmit the MAC cryptogram to the computing device 102, which may then forward the MAC cryptogram to the authentication service 132 for verification as explained below. However, in some embodiments, the computing device 102 may verify the MAC cryptogram.

[0059] More generally, when preparing to send data (e.g., to the server 130 and/or the computing device 436), the contactless card 120 may increment the counter 115. The contactless card 120 may then provide the master key and counter value as input to a cryptographic algorithm, which produces a diversified key 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 AES128; a symmetric HMAC algorithm, such as HMAC-SHA-256; and a symmetric CMAC algorithm such as AES-CMAC.

[0060] The contactless card 120 may then encrypt the data (e.g., the customer identifier and any other data) using the diversified key. The contactless card 432 may then transmit the encrypted data to the computing device 102 (e.g., via an NFC connection, Bluetooth connection, etc.). The computing device 102 may then transmit the encrypted data to the authentication service 132 on the server computing device 130 via the network 106. In at least one embodiment, the contactless card 120 transmits the counter value with the encrypted data. In such embodiments, the contactless card 120 may transmit an encrypted counter value, or an unencrypted counter value.

[0061] Although the counter is used as an example, other data may be used to secure communications between the contactless card 120, the computing device 102, and/or the authentication service 132. For example, the counter may be replaced with a random nonce, generated each time a new diversified key is needed, the full value of a counter value sent from the contactless card 120 and the authentication service 132, a portion of a counter value sent from the contactless card 120 and the authentication service, a counter independently maintained by the contactless card 120 and the authentication service 132 but not sent between the two, a one-time-passcode exchanged between the contactless card 120 and the authentication service 132, and a cryptographic hash of data. In some examples, one or more portions of the diversified key may be used by the parties to create multiple diversified keys.

[0062] Figure 9 depicts a flowchart 900 of steps performed to authenticate the initiating party once the authentication message with the secure package has been received by the authentication service 132 as the recipient party. Initially, the authentication service 132 uses the decryption keys 806 to decrypt the secure package. In addition, the decryption keys 806 are used to decrypt the hash to extract the inputs that were hashed together by the hash function 902. The extracted password and counter value may be compared with the valid password and valid counter value 904. A determination is made whether the passwords match and the counter values match or if the extracted counter value otherwise indicates that the password has not expired 906. If the passwords match and the extracted password has not expired based on the extracted counter value, other extracted information may be compared 908.

[0063] The other information may be other authentication factors 1002, such as depicted in diagram 1000 of Figure 9. The other authentication factors 1002 may include the phone number 1004 of the computing device 102, which may be compared to the phone number on record for the user 118. The other authentication factors 1002 may include a geolocation 1006 for the user 118. The geolocation 1006 may be information such as GPS information or area code and exchange prefix information that may be compared with information regarding the

residence of the user 118. The other authentication factors 1002 may include a shared secret that is shared between the user 118 and the authentication service 132.

[0064] With reference to Figure 9 again, if the other information is valid 910, then the user 118 may be authenticated 914. If not, the user 118 is not authenticated 912. Similarly, if the passwords do not match or the password has expired as indicated by the extracted counter value, the user 118 is not authenticated 912.

[0065] Figure 11 depicts an example of messages that may be exchanged between the user 118 and the programmatic intelligent agent 128 in a successful authentication. First, the user 118 sends an initial message 1120 to the programmatic intelligent agent 128. In this example, the user 118 asks for the routing number of the bank. The programmatic intelligent agent 128 determines that authentication is needed and send a link in a message 1122 to launch code for authentication. The user 118 successfully authenticates, and the programmatic intelligent agent 128 sends a message 1124 indicating that the authentication was successful. In addition, the programmatic intelligent agent 128 sends response message 1126 with the requested routing number.

[0066] Once the user 118 has been successfully authenticated, the user 118 may conduct an authenticated messaging session with the programmatic intelligent agent 128. The programmatic intelligent agent 128 may answer questions of the user 118, provide information to the user 118 and even perform transactions with the user 118, such as financial transactions.

[0067] In order to provide added security, each authenticated messaging session may have an associated expiration time (such as fifteen minutes after starting). This expiration provides an added degree of security to ensure that an imposter has not taken over the session. Moreover, the expiration time ensures that the session does not continue indefinitely with little activity. Such an extended messaging session may pose a security risk.

[0068] Figure 12 depicts a flowchart 1200 of steps that may be performed regarding such expiration times. Initially, the programmatic intelligent agent 128 establishes an expiration time for a newly created authenticated messaging session 1202. The expiration time may be standard amount, such as fifteen minutes after start, or may be tailored to how much traffic is being handled (e.g., shorter expiration times at busy dates/times). The expiration times may even be varied based on the particulars of the customer, like history, location, etc. Eventually, time expires 1204, and the user 118 may be prompted to re-authenticate 1206.

[0069] The programmatic intelligent agent 128 may process data 134 about the user 118 and/or an account of the user 118 to glean insights that may be shared with the user 118. The programmatic intelligent agent 128 may contain pattern matching capabilities and may have

intelligence encoded to react to certain patterns in the data 134. The programmatic intelligent agent 128 may include machine learning capabilities.

[0070] Figure 13 depicts a flowchart 1300 of illustrative steps that may be performed with respect to such processing of the data 134 and informing the user 118 of gleaned insights. The steps depicted in the flowchart 130 are intended to be illustrative and not limiting. Only a few illustrative cases of insights are covered in the flowchart 1300. Initially, the programmatic intelligent agent 128 or a module acting on its behalf processes the data 134 to identify patterns and gain insights 1302. A first pattern that the programmatic intelligent agent may find is one indicative of fraudulent activity 1304. For example, the programmatic intelligent agent may notice that the user 118 shopped at a store that user 118 does not usually shop at or that the store is away from where the user frequents. The programmatic intelligent agent 128 outputs a fraud alert 1306 to the user 118. The fraud alert may, for example, look like the message 1402 of Figure 14A. That message 1402 asks the user if they made a purchase for a given amount at a particular store.

[0071] The programmatic intelligent agent 128 may also check 1306 if there are any unusual patterns in the data that are worth calling to the attention of the user 118. If there are, the programmatic intelligent agent 128 may generate a message that identifies the unusual activity 1310. For example, a message like message 1404 may be generated to note that the spending of the user 118 is up 14% in the latest month. A further pattern that may be identified by the processing of the data is one that indicates that the user 118 is a good candidate for an offer 1312, such as a coupon or an offer for services or a product. Figure 14C, shows an illustrative message that may be generated and sent to the user 118. In this instance, the processing may have indicated that the user is a frequent shopper at Sam's market and would be a good candidate to receive a coupon form Sam's market.

[0072] While the present invention has been described with reference to exemplary embodiments herein, it will be appreciated that various changes in scope and detail may be made without departing from the intended scope as defined in the appended claims.

CLAIMS

1. A method, comprising:
 - receiving a message from a device at a programmatic intelligent agent, the message requesting a response message from the programmatic intelligent agent;
 - determining to perform authentication by contactless card;
 - sending a request message from the programmatic intelligent agent to the device, the request message containing information for launching code to perform the authentication via the contactless card;
 - receiving confirmation at the programmatic intelligent agent that the authentication is successful; and
 - initiating an authenticated messaging session between the device and the programmatic intelligent agent.
2. The method of claim 1, wherein the received message from the device requests access to confidential information or sensitive information.
3. The method of claim 2, comprising generating and sending the response message to the device, wherein the response message contains at least some of the confidential information or at least some of the sensitive information.
4. The method of claim 2, wherein device is associated with a party having a secure account with an institution, and wherein the method further comprises the programmatic intelligent agent accessing the secure account to generate the response message.
5. The method of claim 1, wherein the received message from the device requests a financial transaction.
6. The method of claim 1, wherein the messaging service is a Short Message Service (SMS) messaging service.
7. The method of claim 1, comprising establishing a time limit to the authenticated messaging session such that at expiration of the time limit, the messaging session is no longer authenticated.
8. A non-transitory computer-readable storage medium, the computer-readable storage medium including instructions that when executed by a processor, cause the processor to:

receive a message from a device at a programmatic intelligent agent, the message requesting a response message from the programmatic intelligent agent;
determine to perform authentication by contactless card;
send a request message from the programmatic intelligent agent to the device, the request message containing information for launching code to perform the authentication via the contactless card;
receive confirmation at the programmatic intelligent agent that the authentication is successful; and
initiate an authenticated messaging session between the device and the programmatic intelligent agent.

9. The computer-readable storage medium of claim 8, wherein the received message from the device requests access to confidential information or sensitive information.

10. The computer-readable storage medium of claim 9, comprising the processor further configured to generate and sending the response message to the device, wherein the response message contains at least some of the confidential information or at least some of the sensitive information.

11. The computer-readable storage medium of claim 9, wherein device is associated with a party having a secure account with an institution, and wherein the method further comprises the programmatic intelligent agent access the secure account to generate the response message.

12. The computer-readable storage medium of claim 8, wherein the received message from the device requests a financial transaction.

13. The computer-readable storage medium of claim 8, wherein the messaging service is a Short Message Service (SMS) messaging service.

14. The computer-readable storage medium of claim 8, comprising the processor further configured to establish a time limit to the authenticated messaging session such that at expiration of the time limit, the messaging session is no longer authenticated.

15. A method, comprising:

 sending a message seeking a response message to a programmatic intelligent agent via a messaging service;

receiving a prompt from the programmatic intelligent agent via the messaging service to authenticate an identity via a contactless card;

obtaining information from the contactless card;

forwarding the obtained information to an authenticating authority system to authenticate the identity; and

where the authentication by the authenticating authority is successful, receiving the response message from the programmatic intelligent agent.

16. The method of claim 15, wherein the obtaining information from the contactless card is responsive to the contactless card being in proximity with the device.

17. The method of claim 15, wherein the device includes Near Field Communication (NFC) capabilities and wherein the information is obtained by NFC with the contactless card.

18. The method of claim 15, wherein the obtained information includes credentials and identity information.

19. The method of claim 15, wherein the information is obtained and forwarded in encrypted and/or hashed form.

20. The method of claim 15, further comprising receiving a request message via the messaging service from the programmatic intelligent agent having a link to launch an application on the device for authenticating the identity.

21. The method of claim 15, wherein the message seeking the response message requests information regarding a secure account at a financial institution.

22. The method of claim 15, wherein the message seeking the response message requests a financial transaction.

23. The method of claim 15, wherein the device is a smartphone and wherein the prompt contains a link to launch an application installed on the smartphone to authenticate identity via the contactless card.

24. A non-transitory computer-readable storage medium, the computer-readable storage medium including instructions that when executed by a processor, cause the processor to:

send a message seeking a response message to a programmatic intelligent agent via a messaging service;

receive a prompt from the programmatic intelligent agent via the messaging service to authenticate an identity via a contactless card;

obtain information from the contactless card;

forward the obtained information to an authenticating authority system to authenticate the identity; and

where the authentication by the authenticating authority is successful, receive the response message from the programmatic intelligent agent.

25. The computer-readable storage medium of claim 24, wherein the obtaining information from the contactless card is responsive to the contactless card being in proximity with the device.

26. The computer-readable storage medium of claim 24, wherein the device includes Near Field Communication (NFC) capabilities and wherein the information is obtained by NFC with the contactless card.

27. The computer-readable storage medium of claim 24, wherein the obtained information includes credentials and identity information.

28. The computer-readable storage medium of claim 24, wherein the information is obtained and forwarded in encrypted and/or hashed form.

29. The computer-readable storage medium of claim 24, wherein the instructions further configure the computer to receive a request message via the messaging service from the programmatic intelligent agent having a link to launch an application on the device for authenticating the identity.

30. The computer-readable storage medium of claim 24, wherein the message seek the response message requests information regarding a secure account at a financial institution.

31. The computer-readable storage medium of claim 24, wherein the message seek the response message requests a financial transaction.

32. The computer-readable storage medium of claim 24, wherein the device is a smartphone and wherein the prompt contains a link to launch an application installed on the smartphone to authenticate identity via the contactless card.