



(51) International Patent Classification:

H04L 29/06 (2006.01)

(21) International Application Number:

PCT/US2020/012877

(22) International Filing Date:

09 January 2020 (09.01.2020)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

16/245,813

11 January 2019 (11.01.2019)

US

(71) Applicant: MERCHANT LINK, LLC [US/US]; 8401

Colesville Road, Suite 900, Silver Spring, MD 20910 (US).

(72) Inventors: MCMAHON, Christian, Andreas; 2816 S.

Haven Rd., Annapolis, MD 21401 (US). RYAN, Michael,

Paul; 3207 Winged Elm Dr., Cedar Park, TX 78613 (US).

SHAH, Ketul, Mayurbhai; 693 Ravenwood Dr., Glen

Burnie, MD 21060 (US).

(74) Agent: ROURK, Christopher, J. et al.; Jackson Walker

LLP, 2323 Ross Avenue, Suite 600, Dallas, TX 75201 (US).

(81) Designated States (unless otherwise indicated, for every

kind of national protection available): AE, AG, AL, AM,

AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ,

CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO,

DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN,

HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP,

KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME,
MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ,
OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA,
SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR,
TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every
kind of regional protection available): ARIPO (BW, GH,

GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ,

UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ,

TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK,

EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV,

MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,

TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW,

KM, ML, MR, NE, SN, TD, TG).

Published:

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

(54) Title: SYSTEM AND METHOD FOR SECURE DETOKENIZATION

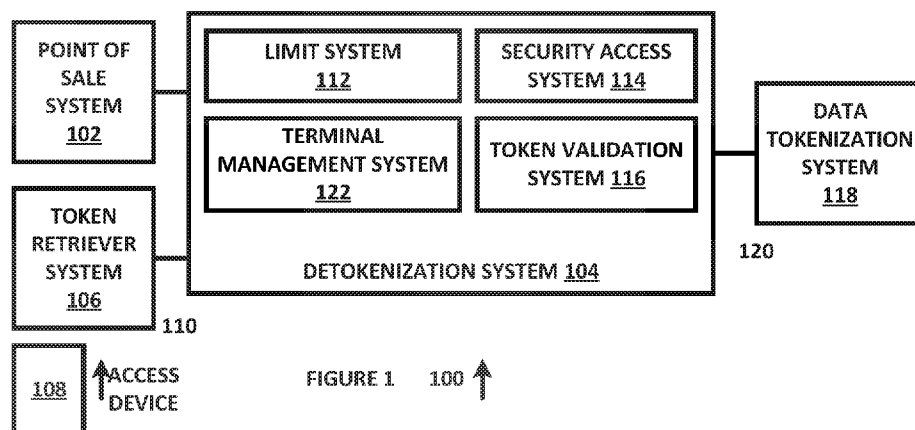


FIGURE 1 100 ↑

(57) Abstract: A system, for accessing protected data comprising a token retriever system operating on a processor and configured to receive a token from a user and to transmit a request, including the token to a detokenization system over a data communications medium. The detokenization system configured to receive the token, to verify that the request has been received from an authorized source, and to transmit a response to the request that includes an account number associated with the token. The token retriever system is configured to receive the account number and to display the account number for a predetermined period of time.



SYSTEM AND METHOD FOR SECURE DETOKENIZATION

TECHNICAL FIELD

[0001] The present disclosure relates generally to data
5 transaction security, and more specifically to a system and
method for secure detokenization of tokenized data.

BACKGROUND OF THE INVENTION

[0002] Converting secure data into an encrypted form to
protect the secure data from misuse is known. For example, U.S.
10 7,451,481, commonly owned and assigned with the pending
application, discloses a database system and method for
encryption and protection of confidential information, and is
hereby incorporated by reference for all purposes as if set
forth herein in its entirety. However, access to the encrypted
15 information in U.S. 7,451,481 by a secure system over a public
network is prevented, to ensure data security.

SUMMARY OF THE INVENTION

[0003] A system for accessing protected data is disclosed
that includes a token retriever system operating on a processor
20 and configured to receive a token from a user and to transmit a
request including the token to a detokenization system over a
data communications medium. The detokenization system is
configured to receive the token, to verify that the request has
been received from an authorized source, and to transmit a
25 response to the request that includes an account number and its
expiration date associated with the token. The token retriever
system is also configured to receive the account number and to
display the account number for a predetermined period of time.

[0004] Other systems, methods, features, and advantages of
30 the present disclosure will be or become apparent to one with
skill in the art upon examination of the following drawings and
detailed description. It is intended that all such additional
systems, methods, features, and advantages be included within

this description, be within the scope of the present disclosure, and be protected by the accompanying claims.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

[0005] Aspects of the disclosure can be better understood with reference to the following drawings. The components in the drawings may be to scale, but emphasis is placed upon clearly illustrating the principles of the present disclosure. Moreover, in the drawings, like reference numerals designate corresponding parts throughout the several views, and in which:

10 **[0006]** FIGURE 1 is a diagram of a system for providing secure detokenization, in accordance with an example embodiment of the present disclosure; and

[0007] FIGURE 2 is a flow chart of an algorithm for providing secure detokenization, in accordance with an example embodiment
15 of the present disclosure.

DETAILED DESCRIPTION OF THE INVENTION

[0008] In the description that follows, like parts are marked throughout the specification and drawings with the same reference numerals. The drawing figures may be to scale and
20 certain components can be shown in generalized or schematic form and identified by commercial designations in the interest of clarity and conciseness.

[0009] **FIGURE 1** is a diagram of a system 100 for providing secure detokenization, in accordance with an example embodiment
25 of the present disclosure. System 100 includes point of sale system 102, token retriever system 106, data tokenization system 118 and detokenization system 104, which further includes limit system 112, security access system 114, token validation system 116 and terminal management system 122, each of which can be
30 implemented in hardware or a suitable combination of hardware and software.

[0010] Point of sale system 102 can be a credit card reader or other suitable device that includes a processor, one or more

memory devices, input/output devices and other components that allow algorithms to be stored in the one or more memory devices and used by the processor to access the input/output devices and to perform algorithmic functions on data received at an input device, to allow processed data to be provided to an output device. Point of sale system 102 includes one or more algorithms that are configured to use a card reader device to read an account number from a credit card with a magnetic stripe, a near field communication (NFC) chip or other suitable security devices and to transmit the account number to a data tokenization system 118 over a public network, such as network 110, for generation of a token. In one example embodiment, the token can be used in place of the account number, such as to eliminate the need for the account number to be made available at point of sale system 102. Because point of sale system 102 can include programmable features and can receive one or more algorithm updates from a remote location to modify the functionality of point of sale system 102, it can be the target of malignant software code (or "malware") that can be used by an unauthorized third party to obtain the account number. Using processes such as those disclosed in U.S. 7,451,481, the account number can be replaced with encrypted data that can be used like a token, to represent the account number for transaction processing. In this manner, the account number can be protected from access by malware, but the account number may be required at a point in the future, such as to resolve a charge dispute. While U.S. 7,451,481 discloses that a centralized encryption and data access system can be used to translate between the encrypted data and the account number, the centralized system cannot be used to address every situation in which the original account number is needed.

[0011] Token retriever system 106 is a portable specialized data processing system that is separate and distinct from point of sale system 102, and can be an Ingenico iWL 252 PIN pad or

other suitable devices that have limited software update functionality. Token retrieval system 106 includes a processor, one or more memory devices, input/output devices and other components that allow algorithms to be stored in the one or more memory devices and used by the processor to access the input/output devices and to perform algorithmic functions on data received at an input device, to allow processed data to be provided to an output device for transmission over a public network such as network 110 to detokenization system 104. In one example embodiment, token retriever system 106 can transmit encoded data that represents a confidential account number (which can be referred to as a "token") to detokenization system 104, and can receive data from detokenization system 104 that represents the account number, an expiration date and other suitable data. The data received from detokenization system 104 can be one or more data packet, data frame or other suitable data structures, can be encrypted and can include other data security protection. Token retriever system 106 can include one or more algorithms that cause the processor of token retriever system 106 to receive and decrypt the one or more data packet or frame to extract the account number, to perform other suitable security processing on the one or more data packet or frame, and then to display the account number associated with the token data for a predetermined period of time, such as 2 minutes. After the period of time has elapsed, the account number can be irrevocably deleted, such as by writing over the data buffer where the account number is stored with a null data set or in other suitable manners. Token retriever system 106 can provide greater security than point of sale system 102, because the ability to modify the algorithms that operate on token retriever system 106 is more limited than the ability to modify the algorithms that operate on point of sale system 102 or other similar systems. In addition, an access device 108 is required to enable token retriever system 106 to operate, such as a card

with encoded identification data stored in a semiconductor memory device, a magnetic stripe or other suitable devices. Access device 108 can be locally authenticated, remotely authenticated or can use other processes to control access to token retriever system 106. Token retriever system 106 can thus be used at different workstations, such as when a bank payment device is not located close to a workstation where a charge is being finalized. In this manner, a user can bring token retriever system 106 to a bank terminal, and eliminates the need to write down account information in an unsecure manner, such as on a note pad.

[0012] Detokenization system 104 includes a processor, one or more memory devices, input/output devices and other components that allow algorithms to be stored in the one or more memory devices and used by the processor to access the input/output devices and to perform algorithmic functions on data received at an input device, to allow processed data to be provided to an output device. Detokenization system 104 can receive a request to detokenize a data string from a token retriever system 106 and can access tokenized data at a data tokenization system 118 over a secure network such as network 120. The data string can include unique numbers that are used to represent credit card account numbers in a system such as U.S. 7,451,481 or other suitable systems, which can be protected behind a secure data network, a firewall system and using other security measures, to prevent a user on a public data network from directly accessing the secure data network. For example, a malicious user on a public data network can send repeated attempts to access a data processing system that is accessible over the public network until access is obtained, and placing data tokenization in systems that cannot be directly accessed over such public networks improves the security of the confidential information that is being tokenized. Thus, while allowing detokenization system 104 to access such data

tokenization systems over a secure network introduces some risk of unauthorized access to the confidential data, detokenization system 104 is configured to provide additional security measures, in addition to firewall protection, access protection and other conventional forms of data security, as discussed herein.

[0013] Limit system 112 operates on the processor of detokenization system 104 or other suitable processors, receives data representing a detokenization request and determines whether a number of detokenization requests exceeds a predetermined threshold. In one example embodiment, the threshold can be implemented as a security measure, and can be based on a number of detokenization requests that would normally be expected for a typical establishment that operates token retriever system 106. In this embodiment, a limit can be established in a hosted system as a security measure to limit an overall detokenization exposure in case of compromise, where the limit can be predetermined and only be changed remotely with a software download to the associated token retriever system 106 or in other suitable manners. Limit system 112 provides additional security by preventing mass detokenization requests from being submitted by a malicious actor, and limits the number of detokenization requests and associated risk of loss, unless additional detokenization requests are requested by an approved operator or using an approved security protocol. In addition, limit system 112 can implement one or more security measures if repeated requests are received from a token retriever system 106 that exceed an allowed number of requests, such as to notify a predetermined user, to shut down operation of the token retriever system 106 or to perform other suitable functions.

[0014] Security access system 114 operates on the processor of detokenization system 104 or other suitable processors, receives data representing a detokenization request and determines whether the detokenization request is from a valid

requester. In one example embodiment, a requester can have an associated access device 108, which can include a card with a near field communications chip, a magnetic stripe or other suitable data storage devices, and token retriever system 106
5 can read encoded data from the data storage device that identifies the location of token retriever system 106, an identifier of the user of access device 108, an identifier of access device 108 and other suitable data that is used to identify token retriever system 106, access device 108 and a
10 user. The user data can be evaluated to determine whether the user is an authorized user for the associated access device 108 and token retriever system 106, such as by using a password, biometric data or other suitable data. User security data processing can also or alternatively be performed locally at
15 token retriever system 106, using a third party system or in other suitable manners. In addition, security access system 114 can implement one or more security measures if repeated requests are received from a token retriever system 106 that do not have a valid source identifier, such as to notify a predetermined
20 user, to shut down operation of the token retriever system 106 or to perform other suitable functions.

[0015] Token validation system 116 operates on the processor of detokenization system 104 or other suitable processors, receives data representing a detokenization request and
25 determines whether the detokenization request is from a valid requester. In one example embodiment, tokenized data can include one or more data fields or combinations of data fields that are used to identify the source of the tokenized data, such as a set of numeric values in predetermined data fields, a
30 predetermined sequence of data or other suitable data. In addition, token validation system 116 can implement one or more security measures if repeated requests are received from a token retriever system 106 that do not have a valid source identifier, such as to notify a predetermined user, to shut down operation

of the token retriever system 106 or to perform other suitable functions. In one example embodiment, a token can be required to pass a local token format check, the token can be verified to determine that it is a validly issued token of detokenization system 104 and is not a token from a third party token, can be
5 verified to ensure that it been issued to a merchant associated with token retriever system 106 (such as where system 100 issues tokens as a function of an individual location or preconfigured group of locations, where the same token does not represent an
10 account number for all merchants but only for a specific merchant and possibly a specific merchant location), the formatting can be checked again at detokenization system 104, and other suitable processes can also or alternatively be used.

[0016] Terminal management system 122 operates on the
15 processor of detokenization system 104 or other suitable processors, and interfaces with token retriever system 106 to provide software updates, security certificate replacement, device health evaluation and other suitable functions. In one example embodiment, terminal management system 122 can
20 periodically query a token retriever system 106 to verify that it has not been tampered with, can request data such as a security certificate, can transmit a new security certificate, can run device operational tests and can perform other suitable functions.

[0017] **FIGURE 2** is a flow chart of an algorithm 200 for
25 providing secure detokenization, in accordance with an example embodiment of the present disclosure. Algorithm 200 can be implemented in hardware or a suitable combination of hardware and software, such as by compiling source code into machine code
30 and then linking the machine code to one or more processors and associated data link libraries, input/output devices, data memory devices and so forth. Although algorithm 200 is shown as a flow chart, it can also or alternatively be implemented as

a state machine, using object-oriented programming or in other suitable manners.

[0018] Algorithm 200 begins at 202, where an access device is received at a token retriever system. In one example embodiment, the access device can be a card having a magnetic stripe, an NFC chip or other suitable data storage devices that are used to identify a specific user, a location associated with the user and other suitable data. The access device data can be periodically updated using a hash or other suitable dynamic data to reduce the risk of misappropriation of the data of the access device. The algorithm then proceeds to 204.

[0019] At 204, it is determined whether a user is authorized. In one example embodiment, the user data can be checked against a local or remote database of users, a remote database of locations where the user is authorized to use a token retriever system, or other suitable data, and additional processes can also or alternatively be used, such as password authentication, biometric authentication, two-step authentication by transmission of an access code to a device of record or other suitable processes. If the user is authorized, the algorithm proceeds to 206, otherwise the algorithm proceeds to 208 where an error message is displayed, such as to the user or to an account administrator.

[0020] At 206, a token is received. In one example embodiment, the token can be manually entered into a data entry device, can be selected from a list of available tokens using a user interface device or can be selected in other suitable manners. The algorithm then proceeds to 210.

[0021] At 210, it is determined whether the source requesting the token has been verified. In one example embodiment, a source can be verified by an IP address, by using physical address data stored at the terminal or in other suitable manners. If the source requesting the token is not verified, the algorithm proceeds to 208, otherwise the algorithm proceeds to 214.

[0022] At 214, it is determined whether the terminal has been verified. In one example embodiment, a terminal can be verified by a terminal identifier, by a software version identifier or in other suitable manners. In another example embodiment, a terminal identifier hosted at a detokenization system or other suitable locations can be required to be enabled before detokenization is performed, such as by determining whether a "detokenization allowed" flag has been set to "on" to enable the functionality of a detokenization system, or in other suitable manners. If the terminal is not verified, the algorithm proceeds to 208, otherwise the algorithm proceeds to 216.

[0023] At 216, it is determined whether the user has been verified. In one example embodiment, a user can be verified by determining whether the user is associated with the token retriever system, with an entity that operates the token retriever system or in other suitable manners. If the user is not verified, the algorithm proceeds to 208, otherwise the algorithm proceeds to 218.

[0024] At 218, it is determined whether a limit on the number of detokenization procedures has been reached. In one example embodiment, each token retriever system can have an associated number of detokenization procedures that it is allowed to perform, such as based on the location of the token retriever system, the historical number of detokenization procedures performed with the token retriever system in a predetermined period of time or in other suitable manners. If the limit has been reached, the algorithm proceeds to 208, otherwise the algorithm proceeds to 220.

[0025] At 220, it is determined whether the token has been verified. In one example embodiment, a token can have a predetermined format, a predetermined relationship between data values in the token or other suitable structural parameters. If the token is not verified, the algorithm proceeds to 208, otherwise the algorithm proceeds to 222.

[0026] At 222, the primary account number is transmitted. In one example embodiment, the token can be transmitted over a secure data network from a detokenization system to a data tokenization system that converted the primary account number into the token, or other suitable processes can be used. Once the primary account number is received at the detokenization system it can be compiled into one or more packets or frames, encrypted and otherwise processed for transmission to a token retriever system or other suitable devices. The algorithm then proceeds to 224.

[0027] At 224, the primary account number is displayed for a predetermined period of time T1. In one example embodiment, a token retriever system can have limited predetermined algorithmic functionality that is installed on a processor and which causes transmitted data to be received, decrypted, reconstructed into a data string having predetermined parameters and displayed on a display for a predetermined period of time. As part of any display, the data may be temporarily stored in a buffer, and after the predetermined time period, the buffer can be purged by storing null data values or in other suitable manners.

[0028] As used herein, the singular forms "a", "an" and "the" are intended to include the plural forms as well, unless the context clearly indicates otherwise. It will be further understood that the terms "comprises" and/or "comprising," when used in this specification, specify the presence of stated features, integers, steps, operations, elements, and/or components, but do not preclude the presence or addition of one or more other features, integers, steps, operations, elements, components, and/or groups thereof. As used herein, the term "and/or" includes any and all combinations of one or more of the associated listed items. As used herein, phrases such as "between X and Y" and "between about X and Y" should be interpreted to include X and Y. As used herein, phrases such as

"between about X and Y" mean "between about X and about Y." As used herein, phrases such as "from about X to Y" mean "from about X to about Y."

[0029] As used herein, "hardware" can include a combination of discrete components, an integrated circuit, an application-specific integrated circuit, a field programmable gate array, or other suitable hardware. As used herein, "software" can include one or more objects, agents, threads, lines of code, subroutines, separate software applications, two or more lines of code or other suitable software structures operating in two or more software applications, on one or more processors (where a processor includes one or more microcomputers or other suitable data processing units, memory devices, input-output devices, displays, data input devices such as a keyboard or a mouse, peripherals such as printers and speakers, associated drivers, control cards, power sources, network devices, docking station devices, or other suitable devices operating under control of software systems in conjunction with the processor or other devices), or other suitable software structures. In one exemplary embodiment, software can include one or more lines of code or other suitable software structures operating in a general purpose software application, such as an operating system, and one or more lines of code or other suitable software structures operating in a specific purpose software application.

As used herein, the term "couple" and its cognate terms, such as "couples" and "coupled," can include a physical connection (such as a copper conductor), a virtual connection (such as through randomly assigned memory locations of a data memory device), a logical connection (such as through logical gates of a semiconducting device), other suitable connections, or a suitable combination of such connections. The term "data" can refer to a suitable structure for using, conveying or storing data, such as a data field, a data buffer, a data message having the data value and sender/receiver address data, a control

message having the data value and one or more operators that cause the receiving system or component to perform a function using the data, or other suitable hardware or software components for the electronic processing of data.

5 **[0030]** In general, a software system is a system that operates on a processor to perform predetermined functions in response to predetermined data fields. For example, a system can be defined by the function it performs and the data fields that it performs the function on. As used herein, a NAME system,
10 where NAME is typically the name of the general function that is performed by the system, refers to a software system that is configured to operate on a processor and to perform the disclosed function on the disclosed data fields. Unless a specific algorithm is disclosed, then any suitable algorithm that would
15 be known to one of skill in the art for performing the function using the associated data fields is contemplated as falling within the scope of the disclosure. For example, a message system that generates a message that includes a sender address field, a recipient address field and a message field would encompass
20 software operating on a processor that can obtain the sender address field, recipient address field and message field from a suitable system or device of the processor, such as a buffer device or buffer system, can assemble the sender address field, recipient address field and message field into a suitable
25 electronic message format (such as an electronic mail message, a TCP/IP message or any other suitable message format that has a sender address field, a recipient address field and message field), and can transmit the electronic message using electronic messaging systems and devices of the processor over a
30 communications medium, such as a network. One of ordinary skill in the art would be able to provide the specific coding for a specific application based on the foregoing disclosure, which is intended to set forth exemplary embodiments of the present disclosure, and not to provide a tutorial for someone having

less than ordinary skill in the art, such as someone who is unfamiliar with programming or processors in a suitable programming language. A specific algorithm for performing a function can be provided in a flow chart form or in other
5 suitable formats, where the data fields and associated functions can be set forth in an exemplary order of operations, where the order can be rearranged as suitable and is not intended to be limiting unless explicitly stated to be limiting.

[0031] It should be emphasized that the above-described
10 embodiments are merely examples of possible implementations. Many variations and modifications may be made to the above-described embodiments without departing from the principles of the present disclosure. All such modifications and variations are intended to be included herein within the scope of this
15 disclosure and protected by the following claims.

What is claimed is:

1. A system for accessing protected data comprising:
a token retriever system operating on a first processor and
5 configured to receive a token from a user and to transmit a
request including the token to a detokenization system over a
data communications medium;
the detokenization system operating on a second processor
and configured to receive the token, to verify that the request
10 has been received from an authorized source, and to transmit a
response to the request that includes an account number
associated with the token; and
wherein the token retriever system is configured to receive
the account number and to display the account number for a
15 predetermined period of time.
2. The system of claim 1 wherein the token retriever
system is configured to receive an access device and to determine
whether the access device is associated with an authorized user.
20
3. The system of claim 1 wherein the detokenization
system further comprises a limit system configured to limit a
number of detokenization procedures from the token retriever
system within a predetermined period of time.
25
4. The system of claim 1 wherein the detokenization
system further comprises a terminal management system configured
to interface with the token retriever system and to authenticate
the token retriever system.
30
5. The system of claim 1 wherein the detokenization
system further comprises a terminal management system configured

to interface with the token retriever system and to replace a security certificate at the token retriever system.

6. The system of claim 1 wherein the detokenization
5 system further comprises a terminal management system configured to interface with the token retriever system and to determine a state of operation of the token retriever system.

7. The system of claim 1 wherein the detokenization
10 system further comprises a security access system configured to interface with the token retriever system and an access device and to determine whether the access device is associated with an authorized user.

8. The system of claim 1 wherein the token retriever
15 system further comprises a first security access system configured to interface with an access device and to determine whether the access device is associated with an authorized user, and the detokenization system further comprises a second
20 security access system configured to interface with the first security access system and the access device and to determine whether the access device is associated with an authorized user.

9. A method for accessing protected data comprising:
25 receiving a token from a user at a token retriever system operating on a first processor;

transmitting a request including the token from the token retriever system to a detokenization system over a data communications medium;

30 receiving the token at the detokenization system;
verifying that the request has been received from an authorized source;

transmitting a response to the request that includes an account number associated with the token; and

receiving the account number at the token retriever system;
and

displaying the account number for a predetermined period
of time.

5

10. The method of claim 9 further comprising:

receiving an access device at the token retriever system;
and

determining whether the access device is associated with
an authorized user.

10

11. The method of claim 9 further comprising limiting a
number of detokenization procedures from the token retriever
system within a predetermined period of time.

15

12. The method of claim 9 further comprising interfacing
with the token retriever system using a terminal management
system to authenticate the token retriever system.

20

13. The method of claim 9 further comprising interfacing
with the token retriever system to replace a security
certificate at the token retriever system.

14. The method of claim 9 further comprising interfacing
with the token retriever system to determine a state of operation
of the token retriever system.

25

15. The method of claim 9 further comprising interfacing
with the token retriever system and an access device to determine
whether the access device is associated with an authorized user.

30

16. The method of claim 9 further comprising:

interfacing with an access device at a detokenization system to determine whether the access device is associated with an authorized user; and

interfacing with the detokenization system and the access
5 device and to determine whether the access device is associated with the authorized user.

17. In a system for accessing protected data having a token retriever system operating on a first processor and
10 configured to receive a token from a user and to transmit a request including the token to a detokenization system over a data communications medium, the detokenization system operating on a second processor and configured to receive the token, to verify that the request has been received from an authorized
15 source, and to transmit a response to the request that includes an account number associated with the token, and wherein the token retriever system is configured to receive the account number and to display the account number for a predetermined period of time, wherein the token retriever system is configured
20 to receive an access device and to determine whether the access device is associated with an authorized user, wherein the detokenization system further comprises a limit system configured to limit a number of detokenization procedures from the token retriever system within a predetermined period of
25 time, wherein the detokenization system further comprises a terminal management system configured to interface with the token retriever system and to authenticate the token retriever system, wherein the terminal management system is configured to interface with the token retriever system and to replace a
30 security certificate at the token retriever system, wherein the terminal management system configured to interface with the token retriever system and to determine a state of operation of the token retriever system, wherein the detokenization system further comprises a security access system configured to

interface with the token retriever system and the access device
and to determine whether the access device is associated with
an authorized user, wherein the token retriever system further
comprises a first security access system configured to interface
5 with the access device and to determine whether the access device
is associated with an authorized user, and the detokenization
system further comprises a second security access system
configured to interface with the first security access system
and the access device and to determine whether the access device
10 is associated with an authorized user, a method for accessing
protected data comprising:

receiving a token from a user at a token retriever system
operating on a first processor;

transmitting a request including the token from the token
15 retriever system to a detokenization system over a data
communications medium;

receiving the token at the detokenization system;

verifying that the request has been received from an
authorized source;

20 transmitting a response to the request that includes an
account number associated with the token;

receiving the account number at the token retriever system;

displaying the account number for a predetermined period
of time;

25 receiving an access device at the token retriever system;

determining whether the access device is associated with
an authorized user;

limiting a number of detokenization procedures from the
token retriever system within a predetermined period of time;

30 interfacing with the token retriever system using a
terminal management system to authenticate the token retriever
system;

interfacing with the token retriever system to replace a
security certificate at the token retriever system;

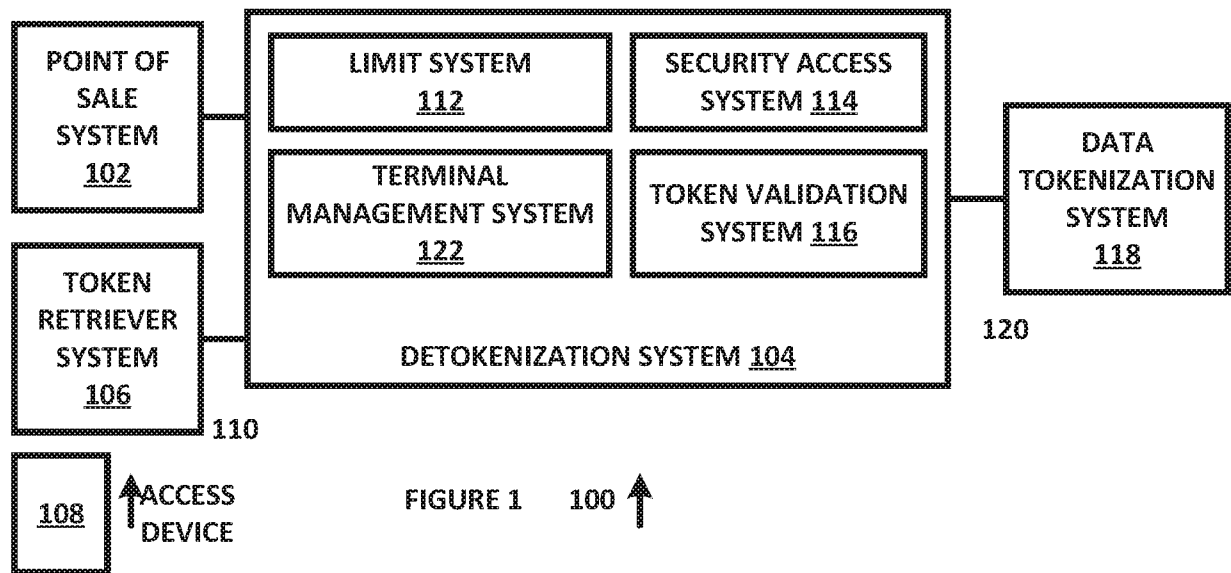
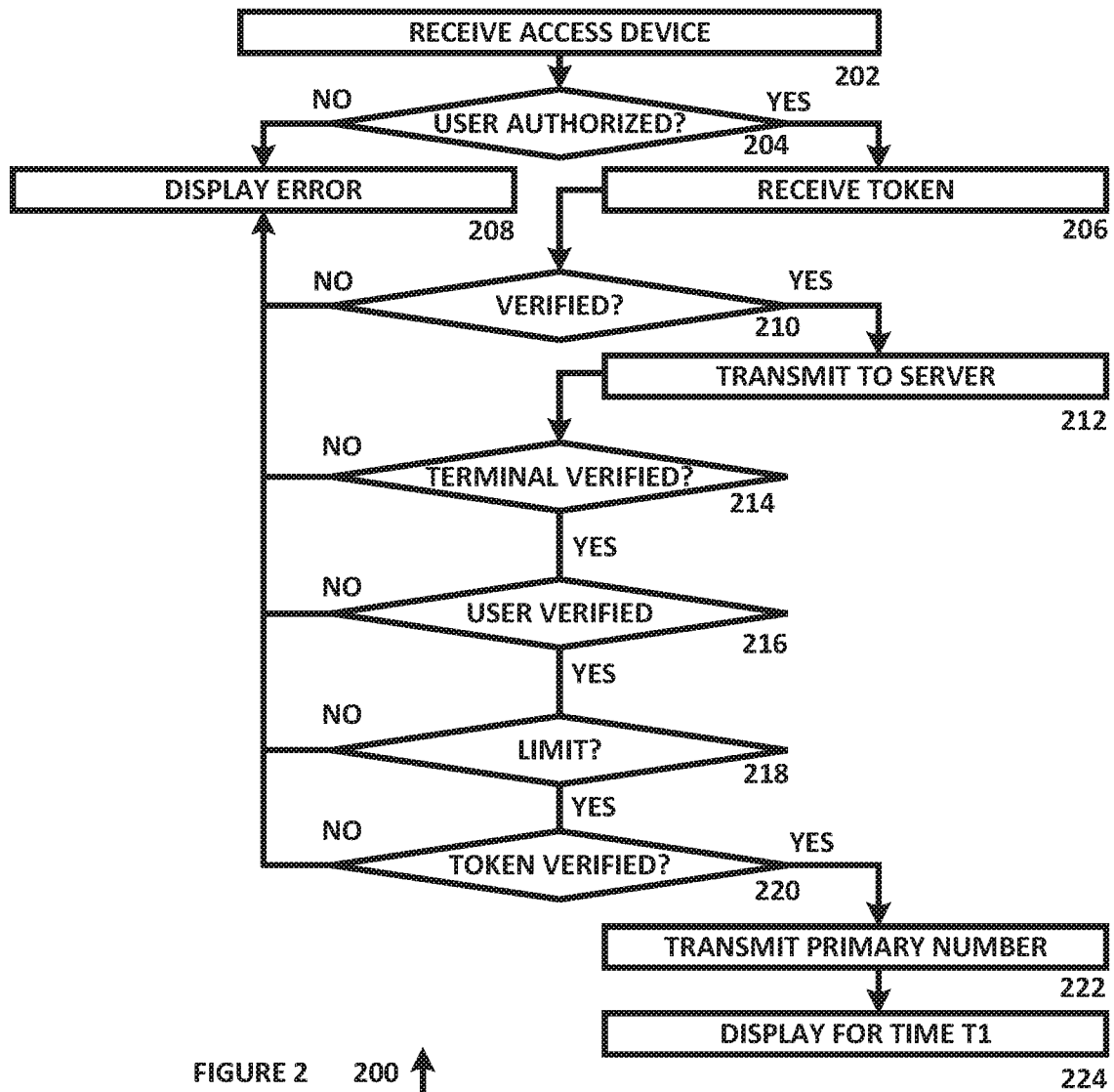
interfacing with the token retriever system to determine a state of operation of the token retriever system;

interfacing with the token retriever system and the access device to determine whether the access device is associated with
5 an authorized user;

interfacing with the access device at a detokenization system to determine whether the access device is associated with the authorized user; and

interfacing with the detokenization system and the access
10 device and to determine whether the access device is associated with the authorized user.

15



INTERNATIONAL SEARCH REPORT

International application No

PCT/US2020/012877

A. CLASSIFICATION OF SUBJECT MATTER
 INV. H04L29/06
 ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2016/119296 A1 (LAXMINARAYANAN PRASANNA [US] ET AL) 28 April 2016 (2016-04-28) paragraph [0093] - paragraph [0105] -----	1-17
X	US 2015/312248 A1 (PRUTHI KAPIL [US] ET AL) 29 October 2015 (2015-10-29) paragraph [0033] - paragraph [0047] -----	1-17
A	US 2018/068297 A1 (GOODMAN DANIEL JASON [US] ET AL) 8 March 2018 (2018-03-08) paragraph [0025] - paragraph [0042] -----	1-17
A	US 2018/268414 A1 (CHUNG KEVIN KWONG-TAI [US] ET AL) 20 September 2018 (2018-09-20) paragraph [0072] - paragraph [0104] -----	1-17



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

6 March 2020

Date of mailing of the international search report

18/03/2020

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
 NL - 2280 HV Rijswijk
 Tel. (+31-70) 340-2040,
 Fax: (+31-70) 340-3016

Authorized officer

Olaechea, Javier

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2020/012877

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2016119296 A1	28-04-2016	US 2016119296 A1	28-04-2016
		US 2018295104 A1	11-10-2018
US 2015312248 A1	29-10-2015	NONE	
US 2018068297 A1	08-03-2018	AU 2017318589 A1	21-02-2019
		CN 109716374 A	03-05-2019
		EP 3507754 A1	10-07-2019
		SG 11201900748Q A	28-03-2019
		US 2018068297 A1	08-03-2018
		WO 2018045134 A1	08-03-2018
US 2018268414 A1	20-09-2018	US 2018268414 A1	20-09-2018
		WO 2018175219 A1	27-09-2018