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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 December 2024 (12.12.2024)

WIPO | PCT

(10) International Publication Number
WO 2024/254350 A2

(51) International Patent Classification:
Not classified

(21) International Application Number:
PCT/US2024/032872

(22) International Filing Date:
06 June 2024 (06.06.2024)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
63/471,296 06 June 2023 (06.06.2023) US

(71) Applicant: **VISA INTERNATIONAL SERVICE ASSOCIATION** [US/US]; P.O. Box 8999, San Francisco, California 94128 (US).

(72) Inventors: **FEDRONIC, Dominique, Louis**; Visa International Service Association, P.O. Box 8999, San Francisco, California 94128 (US). **GUNDAPANENI, Sandeep**; Visa International Service Association, P.O. Box 8999, San Francisco, California 94128 (US). **CHINTHALA, Chandu**; Visa International Service Association, P.O. Box 8999, San Francisco, California 94128 (US).

(74) Agent: **PREPELKA, Nathan, J.** et al.; The Webb Law Firm, One Gateway Center, 420 Ft. Duquesne Blvd., Suite 1200, Pittsburgh, Pennsylvania 15222 (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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, 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.

(54) Title: SYSTEM, METHOD, AND COMPUTER PROGRAM PRODUCT FOR DYNAMICALLY CONTROLLING ACCESS BASED ON UNIQUE ACCESS CRITERIA

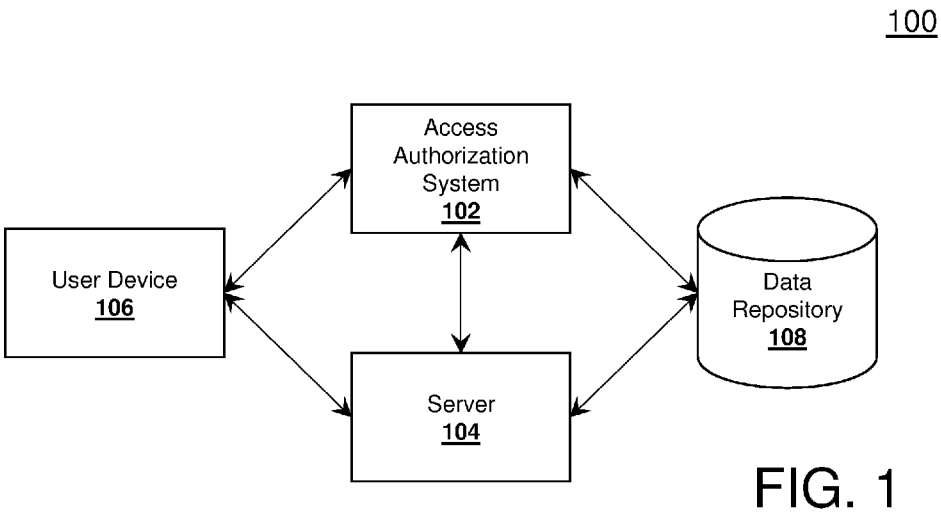

FIG. 1

(57) Abstract: Systems, methods, and computer program products are provided for dynamically controlling access based on unique access criteria. The system includes at least one processor configured to: receive an access request and data associated with a system record, the access request associated with a username of a user, the data associated with the system record comprising a change reason and a change identifier, provision ephemeral credentials to the user based on authenticating the user and based on the data associated with the system record, authorize the user to access at least one target system associated with the access request based on the ephemeral credentials, determine that the user is no longer authorized to access the at least one target system based on the ephemeral credentials, and terminate access to the at least one target system based on determining that the user is no longer authorized to access a production server.

WO 2024/254350 A2

[Continued on next page]

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, 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).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

SYSTEM, METHOD, AND COMPUTER PROGRAM PRODUCT FOR DYNAMICALLY CONTROLLING ACCESS BASED ON UNIQUE ACCESS CRITERIA

CROSS REFERENCE TO RELATED APPLICATION

[0001] This application claims the benefit of United States Provisional Patent Application No. 63/471,296, filed on June 6, 2023, the disclosure of which is hereby incorporated by reference in its entirety.

BACKGROUND

1. Technical Field

[0002] This disclosure relates generally to authorizing access to production systems and, in some non-limiting embodiments or aspects, to systems, methods, and computer program products for dynamically controlling access based on unique access criteria.

2. Technical Considerations

[0003] Some software systems (e.g., software systems at a production level) may require maintenance and/or updates to be performed by privileged users (e.g., users having a range of access and responsible for the development and/or maintenance of a software system). In some instances, privileged users (e.g., privileged users using a client device) may need authorization to a software system that executes (e.g., runs) software applications at a production level (e.g., software applications that are used by customers) via one or more devices (e.g., servers) of the software system. For example, privileged users may receive authorization to access the software system from administrative users (e.g., users having a broad range of access to the software system beyond that of privileged users), granting the privileged user an authorized session on the software system (e.g., on a server of the software system). Alternatively, privileged users may exist initially as non-privileged users (e.g., users having no access to the software system) and the non-privileged users may receive login credentials (e.g., a username and a password) to use in order to authenticate as the privileged user to gain authorized access to the software system. The privileged users may maintain access to the software system as long as the privileged user does not terminate the authorized session (e.g., a login session).

[0004] However, software systems that allow a privileged user to maintain access (e.g., unlimited access, atemporal access, and/or the like) to the software system cannot monitor whether the privileged user is performing actions which may be proper

and/or acceptable to the software system while the privileged user has access to the software system through an authorized session. Sometimes privileged users may misuse the authorized access by performing actions which may be outside a scope of actions that is defined before the privileged user was granted the authorized access. Alternatively, a privileged user may gain authorized access to the software system in order to perform maintenance and/or an update without an intent to misuse the authorized access. The privileged user may perform unintended actions during the course of performing the maintenance and/or update. Managing the scope of authorized access (e.g., permissions) for each privileged user (e.g., of a plurality of privileged users) may become difficult and/or may require a significant amount of resources to maintain and monitor.

[0005] As an example, when a user initiates an interactive session on a Linux server from a Bastion jump-server using a service account, cybersecurity teams cannot efficiently and effectively determine the user that initiated the session.

SUMMARY

[0006] Accordingly, provided are improved systems, methods, and computer program products for dynamically controlling access based on unique access criteria.

[0007] According to non-limiting embodiments or aspects, provided is a computer-implemented method comprising: receiving, with at least one processor, an access request and data associated with a system record, the access request associated with a username of a user, the data associated with the system record comprising a change reason and a change identifier; provisioning, with the at least one processor, ephemeral credentials to the user based on authenticating the user and based on the data associated with the system record; authorizing, with the at least one processor, the user to access at least one target system associated with the access request based on the ephemeral credentials; determining, with the at least one processor, that the user is no longer authorized to access the at least one target system based on the ephemeral credentials; and terminating, with the at least one processor, access to the at least one target system based on determining that the user is no longer authorized to access a production server.

[0008] In non-limiting embodiments or aspects, the method further includes: authenticating, with the at least one processor, the user using multifactor authentication based on the username of the user. In non-limiting embodiments or aspects, the ephemeral credentials are based on a secure shell protocol. In non-

limiting embodiments or aspects, the method further includes: prompting, with the at least one processor, the user to provide the data associated with the system record. In non-limiting embodiments or aspects, the method further includes: validating, with the at least one processor, the data associated with the system record with an initial system record stored in a data repository, wherein validating the data associated with the system record comprises: determining that the data associated with the system record matches master data associated with the initial system record stored in the data repository; and correlating the data associated with the system record with the username of the user based on the master data associated with the initial system record.

[0009] In non-limiting embodiments or aspects, wherein provisioning the ephemeral credentials to the user comprises: determining a duration of time associated with the system record based on the change reason; and generating the ephemeral credentials comprising the duration of time associated with the system record, the duration of time associated with the system record represents a time for which the ephemeral credentials are valid. In non-limiting embodiments or aspects, wherein determining that the user is no longer authorized to access the at least one target system comprises: determining that the duration of time associated with the system record has lapsed. In non-limiting embodiments or aspects, wherein determining that the user is no longer authorized to access the at least one target system comprises: detecting that the user has completed an action associated with the change reason and the change identifier. In non-limiting embodiments or aspects, the ephemeral credentials comprise one or more user role accounts. In non-limiting embodiments or aspects, wherein authorizing the user to access the at least one target system comprises: receiving a request for a connection from the user, the request comprising the ephemeral credentials; determining that the one or more user role accounts of the ephemeral credentials is authorized to access the production server; and initiating a communication session based on the one or more user role accounts, the communication session is configured to transmit one or more messages between a user device of the user and the production server. In non-limiting embodiments or aspects, the method further includes: recording the communication session to generate a recorded communication session; associating the recorded communication session with the username of the user that transmitted the request for the connection; and storing the recorded communication session and the username of the user in a

data repository. In non-limiting embodiments or aspects, the communication session is based on a secure shell protocol.

[0010] In non-limiting embodiments or aspects, the ephemeral credentials comprise a key identifier, the key identifier comprising the username of the user and the change identifier. In non-limiting embodiments or aspects, the method further includes: logging, with the at least one processor, the key identifier, a time of authorization of the user, and a username of at least one user role account of the one or more user role accounts to a log record; storing, with the at least one processor, the key identifier in cache memory of the at least one target system; and retrieving, with the at least one processor, the username of the user of the key identifier from the cache memory of the production server based on a process identifier associated with the at least one target system. In non-limiting embodiments or aspects, wherein authorizing the user to access the at least one target system comprises: receiving a request for a connection, the request comprising the ephemeral credentials; retrieving master data associated with an initial system record stored in a data repository based on the change identifier of the key identifier matching a record identifier of the initial system record; and correlating the at least one target system with the change reason based on an identifier associated with the at least one target system and a change reason of the master data associated with the initial system record. In non-limiting embodiments or aspects, the data repository receives the master data in real-time from a configuration management database. In non-limiting embodiments or aspects, the method further includes generating the ephemeral credentials by digitally signing a user key with a root private key. In non-limiting embodiments or aspects, the method further includes: generating the root private key and corresponding root public key in response to receiving a change request; and distributing the root public key to a subset of production servers including the production server.

[0011] According to non-limiting embodiments or aspects, provided is a system comprising: at least one processor configured to: receive an access request and data associated with a system record, the access request associated with a username of a user, the data associated with the system record comprising a change reason and a change identifier; provision ephemeral credentials to the user based on authenticating the user and based on the data associated with the system record; authorize the user to access at least one target system associated with the access request based on the ephemeral credentials; determine that the user is no longer authorized to access the

at least one target system based on the ephemeral credentials; and terminate access to the at least one target system based on determining that the user is no longer authorized to access a production server.

[0012] In non-limiting embodiments or aspects, the at least one processor is further configured to: authenticate the user using multifactor authentication based on the username of the user. In non-limiting embodiments or aspects, the ephemeral credentials are based on a secure shell protocol. In non-limiting embodiments or aspects, the at least one processor is further configured to: prompt the user to provide the data associated with the system record. In non-limiting embodiments or aspects, the at least one processor is further configured to: validate the data associated with the system record with an initial system record stored in a data repository, wherein validating the data associated with the system record comprises: determining that the data associated with the system record matches master data associated with the initial system record stored in the data repository; and correlating the data associated with the system record with the username of the user based on the master data associated with the initial system record. In non-limiting embodiments or aspects, wherein provisioning the ephemeral credentials to the user comprises: determining a duration of time associated with the system record based on the change reason; and generating the ephemeral credentials comprising the duration of time associated with the system record, the duration of time associated with the system record represents a time for which the ephemeral credentials are valid.

[0013] In non-limiting embodiments or aspects, wherein determining that the user is no longer authorized to access the at least one target system comprises: determining that the duration of time associated with the system record has lapsed. In non-limiting embodiments or aspects, wherein determining that the user is no longer authorized to access the at least one target system comprises: detecting that the user has completed an action associated with the change reason and the change identifier. In non-limiting embodiments or aspects, the ephemeral credentials comprise one or more user role accounts. In non-limiting embodiments or aspects, wherein authorizing the user to access the at least one target system comprises: receiving a request for a connection from the user, the request comprising the ephemeral credentials; determining that the one or more user role accounts of the ephemeral credentials is authorized to access the production server; and initiating a communication session based on the one or more user role accounts, the communication session is configured

to transmit one or more messages between a user device of the user and the production server. In non-limiting embodiments or aspects, the at least one processor is further configured to: record the communication session to generate a recorded communication session; associate the recorded communication session with the username of the user that transmitted the request for the connection; and store the recorded communication session and the username of the user in a data repository. In non-limiting embodiments or aspects, the communication session is based on a secure shell protocol.

[0014] In non-limiting embodiments or aspects, the ephemeral credentials comprise a key identifier, the key identifier comprising the username of the user and the change identifier. In non-limiting embodiments or aspects, the at least one processor is further configured to: log the key identifier, a time of authorization of the user, and a username of at least one user role account of the one or more user role accounts to a log record; store the key identifier in cache memory of the at least one target system; and retrieve the username of the user of the key identifier from the cache memory of the production server based on a process identifier associated with the at least one target system. In non-limiting embodiments or aspects, wherein authorizing the user to access the at least one target system comprises: receiving a request for a connection, the request comprising the ephemeral credentials; retrieving master data associated with an initial system record stored in a data repository based on the change identifier of the key identifier matching a record identifier of the initial system record; and correlating the at least one target system with the change reason based on an identifier associated with the at least one target system and a change reason of the master data associated with the initial system record. In non-limiting embodiments or aspects, the data repository receives the master data in real-time from a configuration management database. In non-limiting embodiments or aspects, the at least one processor is further configured to generating the ephemeral credentials by digitally signing a user key with a root private key. In non-limiting embodiments or aspects, the at least one processor is further configured to: generate the root private key and corresponding root public key in response to receiving a change request; and distribute the root public key to a subset of production servers including the production server.

[0015] According to non-limiting embodiments or aspects, provided is a computer program product comprising at least one non-transitory computer-readable medium

including program instructions that, when executed by at least one processor, cause the at least one processor to: receive an access request and data associated with a system record, the access request associated with a username of a user, the data associated with the system record comprising a change reason and a change identifier; provision ephemeral credentials to the user based on authenticating the user and based on the data associated with the system record; authorize the user to access at least one target system associated with the access request based on the ephemeral credentials; determine that the user is no longer authorized to access the at least one target system based on the ephemeral credentials; and terminate access to the at least one target system based on determining that the user is no longer authorized to access a production server.

[0016] Further non-limiting embodiments or aspects will be set forth in the following numbered clauses:

[0017] Clause 1: A computer-implemented method comprising: receiving, with at least one processor, an access request and data associated with a system record, the access request associated with a username of a user, the data associated with the system record comprising a change reason and a change identifier; provisioning, with the at least one processor, ephemeral credentials to the user based on authenticating the user and based on the data associated with the system record; authorizing, with the at least one processor, the user to access at least one target system based on the ephemeral credentials; determining, with the at least one processor, that the user is no longer authorized to access the at least one target system based on the ephemeral credentials; and terminating, with the at least one processor, access to the at least one target system for which the user was authorized based on determining that the user is no longer authorized to access the at least one target system.

[0018] Clause 2: The computer-implemented method of clause 1, further comprising: authenticating, with the at least one processor, the user using multifactor authentication based on the username of the user.

[0019] Clause 3: The computer-implemented method of clause 1 or 2, wherein the ephemeral credentials are based on a secure shell protocol.

[0020] Clause 4: The computer-implemented method of any of clauses 1-3, further comprising: prompting, with the at least one processor, the user to provide the data associated with the system record.

[0021] Clause 5: The computer-implemented method of any of clauses 1-4, further comprising: validating, with the at least one processor, the data associated with the system record with an initial system record stored in a data repository, wherein validating the data associated with the system record comprises: determining that the data associated with the system record matches master data associated with the initial system record stored in the data repository; and correlating the data associated with the system record with the username of the user based on the master data associated with the initial system record.

[0022] Clause 6: The computer-implemented method of any of clauses 1-5, wherein provisioning the ephemeral credentials to the user comprises: determining a duration of time associated with the system record based on the change reason; and generating the ephemeral credentials comprising the duration of time associated with the system record, wherein the duration of time associated with the system record represents a time for which the ephemeral credentials are valid.

[0023] Clause 7: The computer-implemented method of any of clauses 1-6, wherein determining that the user is no longer authorized to access the at least one target system comprises: determining that the duration of time associated with the system record has lapsed.

[0024] Clause 8: The computer-implemented method of any of clauses 1-7, wherein determining that the user is no longer authorized to access the at least one target system comprises: detecting that the user has completed an action associated with the change reason and the change identifier.

[0025] Clause 9: The computer-implemented method of any of clauses 1-8, wherein the ephemeral credentials comprise one or more user role accounts.

[0026] Clause 10: The computer-implemented method of any of clauses 1-9, wherein authorizing the user to access the at least one target system comprises: receiving a request for a connection from the user, the request comprising the ephemeral credentials; determining that the one or more user role accounts of the ephemeral credentials is authorized to access the at least one target system; and initiating a communication session based on the one or more user role accounts, wherein the communication session is configured to transmit one or more messages between a user device of the user and the production server.

[0027] Clause 11: The computer-implemented method of any of clauses 1-10, further comprising: recording the communication session to generate a recorded

communication session; associating the recorded communication session with the username of the user that transmitted the request for the connection; and storing the recorded communication session and the username of the user in a data repository.

[0028] Clause 12: The computer-implemented method of any of clauses 1-11, wherein the communication session is based on a secure shell protocol.

[0029] Clause 13: The computer-implemented method of any of clauses 1-12, wherein the ephemeral credentials comprise a key identifier, the key identifier comprising the username of the user and the change identifier.

[0030] Clause 14: The computer-implemented method of any of clauses 1-13, further comprising: logging, with the at least one processor, the key identifier, a time of authorization of the user, and a username of at least one user role account of the one or more user role accounts to a log record; storing, with the at least one processor, the key identifier in cache memory of the production server; and retrieving, with the at least one processor, the username of the user of the key identifier from the cache memory of the production server based on a process identifier associated with the production server.

[0031] Clause 15: The computer-implemented method of any of clauses 1-14, wherein authorizing the user to access the production server comprises: receiving a request for a connection, the request comprising the ephemeral credentials; retrieving master data associated with an initial system record stored in a data repository based on the change identifier of the key identifier matching a record identifier of the initial system record; and correlating the production server with the change reason based on an identifier associated with the at least one target system and a change reason of the master data associated with the initial system record.

[0032] Clause 16: The computer-implemented method of any of clauses 1-15, wherein the data repository receives the master data in real-time from a configuration management database.

[0033] Clause 17: The computer-implemented method of any of clauses 1-16, further comprising generating the ephemeral credentials by digitally signing a user key with a root private key.

[0034] Clause 18: The computer-implemented method of any of clauses 1-17, further comprising: generating the root private key and corresponding root public key in response to receiving a change request; and distributing the root public key to a subset of production servers including the production server.

[0035] Clause 19: A system comprising: at least one processor configured to: receive an access request and data associated with a system record, the access request associated with a username of a user, the data associated with the system record comprising a change reason and a change identifier; provision ephemeral credentials to the user based on authenticating the user and based on the data associated with the system record; authorize the user to access at least one target system associated with the access request based on the ephemeral credentials; determine that the user is no longer authorized to access the at least one target system based on the ephemeral credentials; and terminate access to the at least one target system based on determining that the user is no longer authorized to access a production server.

[0036] Clause 20: The system of clause 19, wherein the at least one processor is further configured to: authenticate the user using multifactor authentication based on the username of the user.

[0037] Clause 21: The system of clause 19 or 20, wherein the ephemeral credentials are based on a secure shell protocol.

[0038] Clause 22: The system of any of clauses 19-21, wherein the at least one processor is further configured to: prompt the user to provide the data associated with the system record.

[0039] Clause 23: The system of any of clauses 19-22, wherein the at least one processor is further configured to: validate the data associated with the system record with an initial system record stored in a data repository, wherein validating the data associated with the system record comprises: determining that the data associated with the system record matches master data associated with the initial system record stored in the data repository; and correlating the data associated with the system record with the username of the user based on the master data associated with the initial system record.

[0040] Clause 24: The system of any of clauses 19-23, wherein provisioning the ephemeral credentials to the user comprises: determining a duration of time associated with the system record based on the change reason; and generating the ephemeral credentials comprising the duration of time associated with the system record, wherein the duration of time associated with the system record represents a time for which the ephemeral credentials are valid.

[0041] Clause 25: The system of any of clauses 19-24, wherein determining that the user is no longer authorized to access the at least one target system comprises: determining that the duration of time associated with the system record has lapsed.

[0042] Clause 26: The system of any of clauses 19-25, wherein determining that the user is no longer authorized to access the at least one target system comprises: detecting that the user has completed an action associated with the change reason and the change identifier.

[0043] Clause 27: The system of any of clauses 19-26, wherein the ephemeral credentials comprise one or more user role accounts.

[0044] Clause 28: The system of any of clauses 19-27, wherein authorizing the user to access the at least one target system comprises: receiving a request for a connection from the user, the request comprising the ephemeral credentials; determining that the one or more user role accounts of the ephemeral credentials is authorized to access the production server; and initiating a communication session based on the one or more user role accounts, wherein the communication session is configured to transmit one or more messages between a user device of the user and the production server.

[0045] Clause 29: The system of any of clauses 19-28, wherein the at least one processor is further configured to: record the communication session to generate a recorded communication session; associate the recorded communication session with the username of the user that transmitted the request for the connection; and store the recorded communication session and the username of the user in a data repository.

[0046] Clause 30: The system of any of clauses 19-29, wherein the communication session is based on a secure shell protocol.

[0047] Clause 31: The system of any of clauses 19-30, wherein the ephemeral credentials comprise a key identifier, the key identifier comprising the username of the user and the change identifier.

[0048] Clause 32: The system of any of clauses 19-31, wherein the at least one processor is further configured to: log the key identifier, a time of authorization of the user, and a username of at least one user role account of the one or more user role accounts to a log record; store the key identifier in cache memory of the at least one target system; and retrieve the username of the user of the key identifier from the cache memory of the production server based on a process identifier associated with the at least one target system.

[0049] Clause 33: The system of any of clauses 19-32, wherein authorizing the user to access the at least one target system comprises: receiving a request for a connection, the request comprising the ephemeral credentials; retrieving master data associated with an initial system record stored in a data repository based on the change identifier of the key identifier matching a record identifier of the initial system record; and correlating the at least one target system with the change reason based on an identifier associated with the at least one target system and a change reason of the master data associated with the initial system record.

[0050] Clause 34: The system of any of clauses 19-33, wherein the data repository receives the master data in real-time from a configuration management database.

[0051] Clause 35: The system of any of clauses 19-34 wherein the at least one processor is further configured to generating the ephemeral credentials by digitally signing a user key with a root private key.

[0052] Clause 36: The system of any of clauses 19-35, wherein the at least one processor is further configured to: generate the root private key and corresponding root public key in response to receiving a change request; and distribute the root public key to a subset of production servers including the production server.

[0053] Clause 37: A computer program product comprising at least one non-transitory computer-readable medium including program instructions that, when executed by at least one processor, cause the at least one processor to: receive an access request and data associated with a system record, the access request associated with a username of a user, the data associated with the system record comprising a change reason and a change identifier; provision ephemeral credentials to the user based on authenticating the user and based on the data associated with the system record; authorize the user to access at least one target system associated with the access request based on the ephemeral credentials; determine that the user is no longer authorized to access the at least one target system based on the ephemeral credentials; and terminate access to the at least one target system based on determining that the user is no longer authorized to access a production server.

[0054] These and other features and characteristics of the present disclosure, as well as the methods of operation and functions of the related elements of structures and the combination of parts and economies of manufacture, will become more apparent upon consideration of the following description and the appended claims with reference to the accompanying drawings, all of which form a part of this specification,

wherein like reference numerals designate corresponding parts in the various figures. It is to be expressly understood, however, that the drawings are for the purpose of illustration and description only and are not intended as a definition of the limits of the disclosed subject matter.

BRIEF DESCRIPTION OF THE DRAWINGS

[0055] Additional advantages and details are explained in greater detail below with reference to the non-limiting, exemplary embodiments that are illustrated in the accompanying schematic figures, in which:

[0056] FIG. 1 is a schematic diagram of a system for dynamically controlling access based on unique access criteria according to some non-limiting embodiments or aspects;

[0057] FIG. 2 is a flow diagram of a process for dynamically controlling access based on unique access criteria according to some non-limiting embodiments or aspects;

[0058] FIG. 3 is a diagram of an exemplary environment in which methods, systems, and/or computer program products, described herein, may be implemented according to some non-limiting embodiments or aspects; and

[0059] FIG. 4 is a schematic diagram of example components of one or more devices of FIG. 1 and/or FIG. 3 according to some non-limiting embodiments or aspects.

DETAILED DESCRIPTION

[0060] For purposes of the description hereinafter, the terms “end,” “upper,” “lower,” “right,” “left,” “vertical,” “horizontal,” “top,” “bottom,” “lateral,” “longitudinal,” and derivatives thereof shall relate to the embodiments as they are oriented in the drawing figures. However, it is to be understood that the present disclosure may assume various alternative variations and step sequences, except where expressly specified to the contrary. It is also to be understood that the specific devices and processes illustrated in the attached drawings, and described in the following specification, are simply exemplary and non-limiting embodiments or aspects of the disclosed subject matter. Hence, specific dimensions and other physical characteristics related to the embodiments or aspects disclosed herein are not to be considered as limiting.

[0061] Some non-limiting embodiments or aspects may be described herein in connection with thresholds. As used herein, satisfying a threshold may refer to a value being greater than the threshold, more than the threshold, higher than the threshold,

greater than or equal to the threshold, less than the threshold, fewer than the threshold, lower than the threshold, less than or equal to the threshold, equal to the threshold, etc.

[0062] No aspect, component, element, structure, act, step, function, instruction, and/or the like used herein should be construed as critical or essential unless explicitly described as such. Also, as used herein, the articles “a” and “an” are intended to include one or more items and may be used interchangeably with “one or more” and “at least one.” Furthermore, as used herein, the term “set” is intended to include one or more items (e.g., related items, unrelated items, a combination of related and unrelated items, and/or the like) and may be used interchangeably with “one or more” or “at least one.” Where only one item is intended, the term “one” or similar language is used. Also, as used herein, the terms “has,” “have,” “having,” or the like are intended to be open-ended terms. Further, the phrase “based on” is intended to mean “based at least partially on” unless explicitly stated otherwise. In addition, reference to an action being “based on” a condition may refer to the action being “in response to” the condition. For example, the phrases “based on” and “in response to” may, in some non-limiting embodiments or aspects, refer to a condition for automatically triggering an action (e.g., a specific operation of an electronic device, such as a computing device, a processor, and/or the like).

[0063] As used herein, the term “communication” may refer to the reception, receipt, transmission, transfer, provision, and/or the like of data (e.g., information, signals, messages, instructions, commands, and/or the like). For one unit (e.g., a device, a system, a component of a device or system, combinations thereof, and/or the like) to be in communication with another unit means that the one unit is able to directly or indirectly receive information from and/or transmit information to the other unit. This may refer to a direct or indirect connection (e.g., a direct communication connection, an indirect communication connection, and/or the like) that is wired and/or wireless in nature. Additionally, two units may be in communication with each other even though the information transmitted may be modified, processed, relayed, and/or routed between the first and second unit. For example, a first unit may be in communication with a second unit even though the first unit passively receives information and does not actively transmit information to the second unit. As another example, a first unit may be in communication with a second unit if at least one intermediary unit processes information received from the first unit and communicates

the processed information to the second unit. In some non-limiting embodiments or aspects, a message may refer to a network packet (e.g., a data packet and/or the like) that includes data. It will be appreciated that numerous other arrangements are possible.

[0064] As used herein, the term "computing device" may refer to one or more electronic devices configured to process data. A computing device may, in some examples, include the necessary components to receive, process, and output data, such as a processor, a display, a memory, an input device, a network interface, and/or the like. A computing device may be a mobile device. As an example, a mobile device may include a cellular phone (e.g., a smartphone or standard cellular phone), a portable computer, a wearable device (e.g., watches, glasses, lenses, clothing, and/or the like), a personal digital assistant (PDA), and/or other like devices. A computing device may also be a desktop computer or other form of non-mobile computer.

[0065] As used herein, the term "server" may refer to or include one or more computing devices that are operated by or facilitate communication and processing for multiple parties in a network environment, such as the Internet, although it will be appreciated that communication may be facilitated over one or more public or private network environments and that various other arrangements are possible. Further, multiple computing devices (e.g., servers, point-of-sale (POS) devices, mobile devices, etc.) directly or indirectly communicating in the network environment may constitute a "system."

[0066] As used herein, the term "system" may refer to one or more computing devices or combinations of computing devices (e.g., processors, servers, client devices, software applications, components of such, and/or the like). Reference to "a device," "a server," "a processor," and/or the like, as used herein, may refer to a previously-recited device, server, or processor that is recited as performing a previous step or function, a different device, server, or processor, and/or a combination of devices, servers, and/or processors. For example, as used in the specification and the claims, a first device, a first server, or a first processor that is recited as performing a first step or a first function may refer to the same or different device, server, or processor recited as performing a second step or a second function.

[0067] As used herein, the term "acquirer institution" may refer to an entity licensed and/or approved by a transaction service provider to originate transactions (e.g., payment transactions) using a payment device associated with the transaction service

provider. The transactions the acquirer institution may originate may include payment transactions (e.g., purchases, original credit transactions (OCTs), account funding transactions (AFTs), and/or the like). In some non-limiting embodiments or aspects, an acquirer institution may be a financial institution, such as a bank. As used herein, the term "acquirer system" may refer to one or more computing devices operated by or on behalf of an acquirer institution, such as a server computer executing one or more software applications.

[0068] As used herein, the term "issuer institution" may refer to one or more entities, such as a bank, that provide accounts to customers for conducting transactions (e.g., payment transactions), such as initiating credit and/or debit payments. For example, an issuer institution may provide an account identifier, such as a PAN, to a customer that uniquely identifies one or more accounts associated with that customer. The account identifier may be embodied on a portable financial device, such as a physical financial instrument, e.g., a payment card, and/or may be electronic and used for electronic payments. The term "issuer system" refers to one or more computer devices operated by or on behalf of an issuer institution, such as a server computer executing one or more software applications. For example, an issuer system may include one or more authorization servers for authorizing a transaction.

[0069] As used herein, the term "merchant" may refer to an individual or entity that provides goods and/or services, or access to goods and/or services, to customers based on a transaction, such as a payment transaction. The term "merchant" or "merchant system" may also refer to one or more computer systems operated by or on behalf of a merchant, such as a server computer executing one or more software applications.

[0070] As used herein, the term "payment device" may refer to an electronic payment device, a portable financial device (e.g., a payment card, such as a credit or debit card), a gift card, a smartcard, smart media, a payroll card, a healthcare card, a wristband, a machine-readable medium containing account information, a keychain device or fob, a radio frequency identification (RFID) transponder, a retailer discount or loyalty card, a cellular phone, an electronic wallet mobile application, a PDA, a pager, a security card, a computing device, an access card, a wireless terminal, a transponder, and/or the like. In some non-limiting embodiments or aspects, the payment device may include volatile or non-volatile memory to store information (e.g., an account identifier, a name of the account holder, and/or the like).

[0071] As used herein, the terms "client" and "client device" may refer to one or more client-side devices or systems (e.g., one or more computing devices remote from a transaction service provider) used to initiate or facilitate a transaction (e.g., a payment transaction). As an example, a "client device" may refer to one or more POS devices used by a merchant, one or more acquirer host computers used by an acquirer, one or more mobile devices used by a user, and/or the like. In some non-limiting embodiments or aspects, a client device may be an electronic device configured to communicate with one or more networks and initiate or facilitate transactions. For example, a client device may include one or more computers, portable computers, laptop computers, tablet computers, mobile devices, cellular phones, wearable devices (e.g., watches, glasses, lenses, clothing, and/or the like), PDAs, and/or the like. Moreover, a "client" may also refer to an entity (e.g., a merchant, an acquirer, and/or the like) that owns, utilizes, and/or operates a client device for initiating transactions (e.g., for initiating transactions with a transaction service provider).

[0072] As used herein, the term "transaction service provider" may refer to an entity that receives transaction authorization requests from merchants or other entities and provides guarantees of payment, in some cases through an agreement between the transaction service provider and an issuer institution. For example, a transaction service provider may include a payment network such as Visa® or any other entity that processes transactions. The term "transaction processing system" may refer to one or more computer systems operated by or on behalf of a transaction service provider, such as a transaction processing server executing one or more software applications. A transaction processing server may include one or more processors and, in some non-limiting embodiments or aspects, may be operated by or on behalf of a transaction service provider.

[0073] Non-limiting embodiments or aspects of the disclosed subject matter are directed to systems, methods, and computer program products for authorizing access to computing systems, including, but not limited to, dynamically controlling access based on unique access criteria. Non-limiting embodiments or aspects of the disclosed subject matter may authorize a user (e.g., a privileged user) to access one or more target systems associated with a change request (e.g., production systems, production servers, and/or other systems in scope of a change request, including but not limited to access protected software applications executing on production systems

and/or production servers). Non-limiting embodiments or aspects of the disclosed subject matter may control (e.g., customize, dynamically change, and/or the like) the authorization of the user based on a plurality of factors. For example, non-limiting embodiments or aspects of the disclosed subject matter may authorize the user to access a target system, such as a production server, for a predetermined duration of time (e.g., a window of time). Non-limiting embodiments or aspects of the disclosed subject matter may terminate access authorized to the user based on detecting that the user has completed an action (e.g., an intended action, a documented action, a recorded action, and/or the like) on the production server (e.g., an application executing on the production server). Additionally, non-limiting embodiments or aspects of the disclosed subject matter may determine (e.g., track, record, and/or the like) a username of the user (e.g., corresponding to the user) that the user used (e.g., that the user was signed into) when the user was authorized to access the production server. Non-limiting embodiments or aspects of the disclosed subject matter may validate the authorization of the user to access the production server against data associated with a change control management system (e.g., change control data, data associated with change requests (CRQs), and/or the like).

[0074] Non-limiting embodiments or aspects of the disclosed subject matter may authorize users to access a target system in real-time without requiring a user to have specific login information associated with a privileged account and/or an administrative account. Additionally, once a user is authorized access to a target system, non-limiting embodiments or aspects of the disclosed subject matter may detect when a user performs an authorized and/or an unauthorized action and non-limiting embodiments or aspects may terminate the authorization of the user to access the target system in real-time (e.g., within seconds or milliseconds such that it is substantially imperceptible to the user) when the user performs an unauthorized action. Non-limiting embodiments or aspects of the disclosed subject matter may automate the approval and provisioning of authorization of the user to access the target system by leveraging a data repository storing a plurality of data associated with the change control management system (e.g., a plurality of data associated with change requests and/or the like). In this way, non-limiting embodiments or aspects of the disclosed subject matter may align (e.g., control) the provisioning of authorization to users to access target systems with requirements for a change and/or fixing an incident associated with a target system such that the user is only authorized access to a system (e.g., to

parts of a production system, to software applications of a production system, and/or the like) that is within the scope of the change and/or the requirement to fix the incident. Thus, non-limiting embodiments or aspects of the disclosed subject matter may prevent unauthorized changes and/or tampering with target systems, even by users who may be authorized to access the system for a proper purpose. Thus, non-limiting embodiments or aspects of the disclosed subject matter may dynamically control a user's authorization and/or access to target systems based on unique criteria that outlines the amount of access that the user may require to perform a specific action and/or task. Non-limiting embodiments or aspects also provide for traceability by mapping the activity of an authorized principal to the user in real-time (e.g., while the user is making changes), even when multiple users are concurrently active with the same authorized principal (e.g., a shared principal entity) on the same server. Non-limiting embodiments or aspects described herein may be used to provide privileged access to a UNIX-based system, although it will be appreciated that non-limiting embodiments may be used to provide access to various types of systems.

[0075] Referring now to FIG. 1, shown is a system 100 for dynamically controlling access based on unique access criteria according to some non-limiting embodiments or aspects. The system 100 may include access authorization system 102, server 104, user device 106, and data repository 108.

[0076] Access authorization system 102 may include a computing device, such as a server (e.g., a single server), a group of servers, and/or other like devices. In some non-limiting embodiments or aspects, access authorization system 102 may include a processor and/or memory, as described herein. In some non-limiting embodiments or aspects, access authorization system 102 may include one or more software instructions (e.g., one or more software applications) executing on a server (e.g., a single server), a group of servers, a computing device (e.g., a single computing device), a group of computing devices, and/or other like devices. In some non-limiting embodiments or aspects, access authorization system 102 may be configured to communicate with server 104, user device 106, and/or data repository 108. In some non-limiting embodiments or aspects, access authorization system 102 may be in communication with server 104, user device 106, and/or data repository 108 such that access authorization system 102 is separate from server 104, user device 106, and/or data repository 108. In some non-limiting embodiments or aspects, server 104, user

device 106, and/or data repository 108 may be implemented by (e.g., may be part of) access authorization system 102.

[0077] Server 104 may include at least one server, computing device, and/or at least one processor (e.g., a multi-core processor), such as a central processing unit (CPU), an accelerated processing unit (APU), a graphics processing unit (GPU), a microprocessor, and/or the like. In some non-limiting embodiments or aspects, server 104 may be programmed to perform one or more steps of methods described herein. In some non-limiting embodiments or aspects, server 104 may be in communication with one or more user devices 106. In some non-limiting embodiments or aspects, server 104 may be configured to receive information from and/or communicate (e.g., transmit) information to access authorization system 102, one or more user devices 106, one or more other servers 104, and/or data repository 108. In some non-limiting embodiments or aspects, server 104 may execute an instance (e.g., an instance of a software application) of access authorization system 102. In some non-limiting embodiments or aspects, server 104 may be implemented by (e.g., may be part of) access authorization system 102. In other examples, server 104 may be in communication with access authorization system 102 such that server 104 is separate from access authorization system 102.

[0078] In non-limiting embodiments or aspects, user device 106 may include a computing device configured to communicate with access authorization system 102 and/or server 104 via a communication network. For example, user device 106 may include a computing device, such as a desktop computer, a portable computer (e.g., tablet computer, a laptop computer, and/or the like), a mobile device (e.g., a cellular phone, a smartphone, a personal digital assistant, a wearable device, and/or the like), and/or other like devices. In some non-limiting embodiments or aspects, user device 106 may be associated with a user (e.g., an individual operating user device 106). In some non-limiting embodiments or aspects, user device 106 may be implemented by (e.g., may be part of) access authorization system 102. In some examples, user device 106 may be in communication with access authorization system 102 and/or server 104 such that user device 106 is separate from access authorization system 102 and/or server 104.

[0079] In non-limiting embodiments or aspects, data repository 108 may include a computing device (e.g., a database device) configured to communicate with access authorization system 102 and/or server 104 via a communication network. For

example, data repository 108 may include a server, a group of servers, and/or other like devices. In some non-limiting embodiments or aspects, data repository 108 may be associated with one or more computing devices providing interfaces, such that a user (e.g., an administrative user) may interact with data repository 108 via the one or more computing devices. Data repository 108 may be in communication with access authorization system 102 and/or server 104 such that data repository 108 is separate from access authorization system 102 and/or server 104. In other examples, data repository 108 may be implemented by (e.g., may be part of) access authorization system 102, server 104, and/or user device 106.

[0080] The number and arrangement of systems and devices shown in FIG. 1 are provided as an example. There may be additional systems and/or devices, fewer systems and/or devices, different systems and/or devices, and/or differently arranged systems and/or devices than those shown in FIG. 1. Furthermore, two or more systems or devices shown in FIG. 1 may be implemented within a single system or device, or a single system or device shown in FIG. 1 may be implemented as multiple, distributed systems or devices. Additionally or alternatively, a set of systems (e.g., one or more systems) or a set of devices (e.g., one or more devices) of system 100 may perform one or more functions described as being performed by another set of systems or another set of devices of system 100.

[0081] Referring now to FIG. 2, shown is a process 200 for dynamically controlling access based on unique access criteria according to some non-limiting embodiments or aspects. The steps shown in FIG. 2 are for example purposes only. It will be appreciated that additional, fewer, different, and/or a different order of steps may be used in non-limiting embodiments or aspects.

[0082] As shown in FIG. 2, at step 202, process 200 may include receiving an access request from a user. For example, access authorization system 102 may receive an access request and data associated with a system record from a user. In non-limiting embodiments, the request is for a credential for any server and/or system in the scope of an incident or change request (e.g., as indicated by a change identifier and/or incident identifier). For example, an incident or change request may be mapped to one or more systems that host and/or manage one or more applications, development environments, tools, operating systems, and/or the like. In some non-limiting embodiments or aspects, the access request may be for an SSH (Secure Shell) certificate (e.g., for SSH certificate-based authentication) and/or another type of

public/private key pair authentication schema. In some non-limiting embodiments or aspects, the access request may be associated with a username of the user that transmitted the access request to access authorization system 102. In some non-limiting embodiments or aspects, the data associated with the system record may include a change reason and a change identifier. In some non-limiting embodiments or aspects, access authorization system 102 may prompt the user to provide the data associated with the system record and access authorization may receive the data associated with the system record from user device 106 associated with the user.

[0083] In some non-limiting embodiments or aspects, access authorization system 102 may validate the data associated with the system record with an initial system record. In some non-limiting embodiments or aspects, a plurality of initial system records may be stored in data repository 108. The plurality of initial system records may include the initial system record. In some non-limiting embodiments or aspects, access authorization system 102 may validate the data associated with the system record by determining that the data associated with the system record matches master data associated with the initial system record stored in data repository 108. In some non-limiting embodiments or aspects, access authorization system 102 may validate the data associated with the system record by correlating the data associated with the system record with the username of the user based on the master data associated with the initial system record.

[0084] As shown in FIG. 2, at step 204, process 200 may include provisioning credentials to the user. For example, access authorization system 102 may provision ephemeral credentials (e.g., credentials that are valid for a limited time and/or purpose) to the user (e.g., the user that transmitted the access request) based on authenticating the user and based on the data associated with the system record. In some non-limiting embodiments or aspects, the ephemeral credentials may be based on a secure shell protocol. For example, access authorization system 102 may use the ephemeral credentials to authorize a session (e.g., a communication session) between a server and a client device based on the secure shell protocol. In some non-limiting embodiments or aspects, the ephemeral credentials may include one or more user role accounts (e.g., a list of one or more user role accounts associated with the ephemeral credentials).

[0085] In non-limiting embodiments or aspects, the credentials are generated by a credentialing service (e.g., associated with a Certificate Authority (CA)) that generates

an SSH certificate, as an example, by digitally signing a public key of the user with a private key of the CA. The public key corresponding to the private key of the CA may be distributed to target production systems. In non-limiting embodiments, the credentialing service may include a frontend client and a backend service, where the frontend client is on the user device and prompts the users for a valid change and/or incident and forwards the credential request to the backend service, and where the backend service receives the request and validates whether the change and/or incident is valid. The SSH certificate used as an ephemeral credential may be associated with and/or include a list of authorized principals (e.g., authorized administrative entities), such that a user with the SSH certificate can only impersonate or act in the capacity of those listed authorized principals.

[0086] In some non-limiting embodiments or aspects, access authorization system 102 may authenticate the user using multifactor authentication. In some non-limiting embodiments or aspects, access authorization system 102 may authenticate the user based on the username of the user. In some non-limiting embodiments or aspects, the ephemeral credentials may include a key identifier (e.g., a key identifier associated with the ephemeral credentials). In some non-limiting embodiments or aspects, the key identifier may include the username of the user and the change identifier (e.g., the username of the user concatenated with the change identifier). However, it will be appreciated that the key identifier may include any unique identifier such as a string of characters and/or the like.

[0087] In non-limiting embodiments, the ephemeral credential is used to open a session and may no longer be involved as the session progresses. The session may be terminated at the same time that the credential is set to expire.

[0088] In some non-limiting embodiments or aspects, access authorization system 102 may log (e.g., record and/or track in a log record stored on a recording medium, such as a data storage device) the key identifier, a time of authorization of the user, and a username of at least one user role account of the one or more user role accounts. In some non-limiting embodiments or aspects, access authorization system 102 may store the key identifier in cache memory of a production server and/or other system. In some non-limiting embodiments or aspects, access authorization system 102 may retrieve the username of the user of (e.g., included in) the key identifier from the cache memory of the production server and/or other system based on a process identifier associated with the production server and/or other system.

[0089] In some non-limiting embodiments or aspects, access authorization system 102 may provision the ephemeral credentials to the user, the ephemeral credentials including a duration of time associated with the system record. For example, access authorization system 102 may determine the duration of time associated with the system record based on the change reason. In some non-limiting embodiments or aspects, access authorization system 102 may assign the duration of time to the ephemeral credentials. In some non-limiting embodiments or aspects, access authorization system 102 may generate the ephemeral credentials including the duration of time associated with the system record. In some non-limiting embodiments or aspects, the duration of time associated with the system record may represent a time for which the ephemeral credentials are valid. In non-limiting embodiments, access authorization system 102 may provision ephemeral credentials that are unique to the user and a jump-server and/or bastion host used for protecting ports in a public network.

[0090] As shown in FIG. 2, at step 206, process 200 may include authorizing the user to access a target system (e.g., production system and/or other system). For example, in some non-limiting embodiments or aspects, access authorization system 102 may authorize the user to access the production server and/or other system based on the ephemeral credentials (e.g., based on access authorization system 102 accepting the ephemeral credentials as valid credentials). In some non-limiting embodiments or aspects, access authorization system 102 may authorize the user to access the production server and/or other system by receiving a request for a connection from the user. In some non-limiting embodiments or aspects, the request may include the ephemeral credentials. In some non-limiting embodiments or aspects, access authorization system 102 may authorize the user to access the production server and/or other system by determining that the one or more user role accounts of the ephemeral credentials (e.g., the list of one or more user role accounts associated with the ephemeral credentials) is authorized to access the production server and/or other system.

[0091] In some non-limiting embodiments or aspects, access authorization system 102 may authorize the user to access the production server and/or other system by receiving a request for a connection. In some non-limiting embodiments or aspects, the request may include the ephemeral credentials. In some non-limiting embodiments or aspects, access authorization system 102 may authorize the user to

access the production server and/or other system by retrieving master data associated with an initial system record stored in data repository 108. Access authorization system 102 may retrieve the master data based on the change identifier of (e.g., included in) the key identifier matching a record identifier of the initial system record (e.g., an initial system record identifier, such as an integer). In some non-limiting embodiments or aspects, access authorization system 102 may authorize the user to access the production server and/or other system by correlating the production server and/or other system with the change reason based on the identifier associated with the production server and/or other system and a change reason of the master data associated with the initial system record. In some non-limiting embodiments or aspects, data repository 108 may receive the master data (e.g., master data associated with a plurality of initial system records) in real-time from a configuration management database (e.g., ServiceNow®).

[0092] In some non-limiting embodiments or aspects, access authorization system 102 may initiate a communication session based on the one or more user role accounts (e.g., during and/or after access authorization system 102 authorizes the user to access the production server and/or other system). In some non-limiting embodiments or aspects, the communication session may be configured to transmit one or more messages between a user device of the user and the production server and/or other system. In some non-limiting embodiments or aspects, the communication session may be based on a secure shell protocol.

[0093] In non-limiting embodiments, an authorized principal command on every target host is configured to resolve whether a given authorized principal is allowed to access the target host. Every login using the ephemeral credential automatically triggers the authorized principal command, such that the list of authorized principal(s) is returned and can be checked against the authorized principal(s) in the ephemeral credential. If there is no match, authentication is denied. The authorized principal command may have access to incoming credential details such as the key identifier, and may use the key identifier to query, in real-time (e.g., within seconds or milliseconds such that it is substantially imperceptible to the user), a data structure that includes the scope of change and/or incident request to determine whether the scope includes the current server/host. The list of authorized principals may be returned by the authorized principal command in response to determining that the

scope includes the current server/host. Otherwise, the command may return null or empty authorized principals, denying authorization.

[0094] In some non-limiting embodiments or aspects, access authorization system 102 may record the communication session to generate a recorded communication session. In some non-limiting embodiments or aspects, access authorization system 102 may associate the recorded communication session with the username of the user that transmitted the request for the connection. In some non-limiting embodiments or aspects, access authorization system 102 may store the recorded communication session and the username of the user in data repository 108. For example, access authorization system 102 may store the recorded communication session with the username of the user that is associated with the recorded communication session such that the recorded communication session and the username of the user are associated in data repository 108.

[0095] As shown in FIG. 2, at step 208, process 200 may include determining that the user is not authorized to access the target system and/or other system. For example, in some non-limiting embodiments or aspects, access authorization system 102 may determine that the user is not authorized (e.g., no longer authorized after previously being authorized) to access the target system based on the ephemeral credentials. In some non-limiting embodiments or aspects, access authorization system 102 may determine that the user is not authorized to access the target system based on determining that the duration of time associated with the system record has lapsed. In some non-limiting embodiments or aspects, access authorization system 102 may determine that the user is not authorized to access the target system on detecting that the user has completed an action associated with the change reason and the change identifier.

[0096] As shown in FIG. 2, at step 210, process 200 may include terminating access to the target system(s) (e.g., terminating the user's access to the target system(s), terminating the access previously granted to the user, and/or the like). For example, in some non-limiting embodiments or aspects, access authorization system 102 may terminate access (e.g., the user's access) to the production server and/or other system for which the user was authorized based on determining that the user is not authorized to access the production server and/or other system.

[0097] In non-limiting embodiments or aspects, the CA public key (e.g., the CA public key that may be distributed to target systems as an initial set-up step) may be

ephemeral in addition to the ephemeral credential (e.g., an SSH certificate) issued to the user. For example, a credentialing service may generate an ephemeral public/private key pair (e.g., a "CA root key") in response to a change request, and distribute the ephemeral CA root public key to only the target systems (e.g., hosts, production servers, and/or other systems) that are in scope for the change request. For example, a list of servers (e.g., production systems or hosts) to which the change may apply is often a small subset of all the servers in scope of the final change (e.g., only servers in one data center may be in scope of a particular change request so that if an error occurs the service can be provided by servers in other data centers). In some examples, changes may be made to one data center at a time to deploy a final change across systems.

[0098] In such an example, the ephemeral credential generated for the user may be signed with the CA root private key that corresponds to the CA root public key. With such an arrangement, the ephemeral credential provisioned to the user (e.g., an SSH certificate or the like) will only be valid to access production systems or hosts that are in the scope of the change request. This provides an enforcement mechanism to ensure that any users performing the change will not extend the scope of the change to production systems or hosts that were not approved to be in the change. This removes a vector of a potential security breach and avoids unintended outages.

[0099] In non-limiting embodiments, unauthorized lateral access may be prevented and detected. For example, every successful SSH connection (e.g., port 22 or the like) from any production systems (production hosts) may be monitored by a script that is configured to extract information such as source user, source port, destination host, destination port, and/or the like. That information may be logged (e.g., in a sold-state hybrid drive (SSHD) or the like). In this manner, SSH client data (e.g., timestamp, target host/server, source host, port, user identifier, and/or the like) may be correlated to logged data, using the timestamp, source post, port, and target server/host, as examples, for the key between the two different data sources to determine when a user logged onto which monitored service identifier and from which source server to which target server. Both data sources may then be input into a monitoring and alerting system. The alerts may be input into a data lake (e.g., via Hadoop or the like) and processed by one or more anomaly detection algorithms (e.g., such as a machine-learning algorithm or the like). The monitoring and alerting may prevent and detect lateral access even in the absence of micro segmentation.

[0100] Non-limiting embodiments described herein may be used to seamlessly control a user's access to production systems with approved change or valid incident windows by leveraging the enterprise change management system in substantially real-time (e.g., within seconds or milliseconds such that it is substantially imperceptible to the user). This improves security, improves user productivity, and offers frictionless production access when needed, by seamlessly automating the integration of complex systems.

[0101] Referring now to FIG. 3, shown is a diagram of a non-limiting embodiment or aspect of an exemplary environment 300 in which systems, products, and/or methods, as described herein, may be implemented. As shown in FIG. 3, environment 300 may include transaction service provider system 302, issuer system 304, customer device 306, merchant system 308, acquirer system 310, and communication network 312. In some non-limiting embodiments or aspects, each of access authorization system 102, server 104, user device 106, and/or data repository 108 may be implemented by (e.g., may be part of) transaction service provider system 302. In some non-limiting embodiments or aspects, at least one of each of access authorization system 102, server 104, user device 106, and/or data repository 108 may be implemented by (e.g., may be part of) another system, another device, another group of systems, or another group of devices, separate from or including transaction service provider system 302, such as issuer system 304, merchant system 308, acquirer system 310, and/or the like.

[0102] Transaction service provider system 302 may include one or more devices capable of receiving information from and/or communicating information to issuer system 304, customer device 306, merchant system 308, and/or acquirer system 310 via communication network 312. For example, transaction service provider system 302 may include a computing device, such as a server (e.g., a transaction processing server), a group of servers, and/or other like devices. In some non-limiting embodiments or aspects, transaction service provider system 302 may be associated with a transaction service provider as described herein. In some non-limiting embodiments or aspects, transaction service provider system 302 may be in communication with a data storage device (e.g., data repository 108), which may be local or remote to transaction service provider system 302. In some non-limiting embodiments or aspects, transaction service provider system 302 may be capable of

receiving information from, storing information in, communicating information to, or searching information stored in the data storage device.

[0103] Issuer system 304 may include one or more devices capable of receiving information and/or communicating information to transaction service provider system 302, customer device 306, merchant system 308, and/or acquirer system 310 via communication network 312. For example, issuer system 304 may include a computing device, such as a server, a group of servers, and/or other like devices. In some non-limiting embodiments or aspects, issuer system 304 may be associated with an issuer institution as described herein. For example, issuer system 304 may be associated with an issuer institution that issued a credit account, debit account, credit card, debit card, and/or the like to a user associated with customer device 306.

[0104] Customer device 306 may include one or more devices capable of receiving information from and/or communicating information to transaction service provider system 302, issuer system 304, merchant system 308, and/or acquirer system 310 via communication network 312. Additionally or alternatively, each customer device 306 may include a device capable of receiving information from and/or communicating information to other customer devices 306 via communication network 312, another network (e.g., an ad hoc network, a local network, a private network, a virtual private network, and/or the like), and/or any other suitable communication technique. For example, customer device 306 may include a client device and/or the like. In some non-limiting embodiments or aspects, customer device 306 may or may not be capable of receiving information (e.g., from merchant system 308 or from another customer device 306) via a short-range wireless communication connection (e.g., an NFC communication connection, an RFID communication connection, a Bluetooth® communication connection, a Zigbee® communication connection, and/or the like), and/or communicating information (e.g., to merchant system 308) via a short-range wireless communication connection.

[0105] Merchant system 308 may include one or more devices capable of receiving information from and/or communicating information to transaction service provider system 302, issuer system 304, customer device 306, and/or acquirer system 310 via communication network 312. Merchant system 308 may also include a device capable of receiving information from customer device 306 via communication network 312, a communication connection (e.g., an NFC communication connection, an RFID communication connection, a Bluetooth® communication connection, a Zigbee®

communication connection, and/or the like) with customer device 306, and/or the like, and/or communicating information to customer device 306 via communication network 312, the communication connection, and/or the like. In some non-limiting embodiments or aspects, merchant system 308 may include a computing device, such as a server, a group of servers, a client device, a group of client devices, and/or other like devices. In some non-limiting embodiments or aspects, merchant system 308 may be associated with a merchant as described herein. In some non-limiting embodiments or aspects, merchant system 308 may include one or more client devices. For example, merchant system 308 may include a client device that allows a merchant to communicate information to transaction service provider system 302. In some non-limiting embodiments or aspects, merchant system 308 may include one or more devices, such as computers, computer systems, and/or peripheral devices capable of being used by a merchant to conduct a transaction with a user.

[0106] Acquirer system 310 may include one or more devices capable of receiving information from and/or communicating information to transaction service provider system 302, issuer system 304, customer device 306, and/or merchant system 308 via communication network 312. For example, acquirer system 310 may include a computing device, a server, a group of servers, and/or the like. In some non-limiting embodiments or aspects, acquirer system 310 may be associated with an acquirer as described herein.

[0107] Communication network 312 may include one or more wired and/or wireless networks. For example, communication network 312 may include a cellular network (e.g., a long-term evolution (LTE®) network, a third generation (3G) network, a fourth generation (4G) network, a fifth generation (5G) network, a code division multiple access (CDMA) network, and/or the like), a public land mobile network (PLMN), a local area network (LAN), a wide area network (WAN), a metropolitan area network (MAN), a telephone network (e.g., the public switched telephone network (PSTN)), a private network (e.g., a private network associated with a transaction service provider), an ad hoc network, an intranet, the Internet, a fiber optic-based network, a cloud computing network, and/or the like, and/or a combination of these or other types of networks.

[0108] The number and arrangement of systems, devices, and/or networks shown in FIG. 3 are provided as an example. There may be additional systems, devices, and/or networks; fewer systems, devices, and/or networks; different systems, devices, and/or networks; and/or differently arranged systems, devices, and/or networks than

those shown in FIG. 3. Furthermore, two or more systems or devices shown in FIG. 3 may be implemented within a single system or device, or a single system or device shown in FIG. 3 may be implemented as multiple, distributed systems or devices. Additionally or alternatively, a set of systems (e.g., one or more systems) or a set of devices (e.g., one or more devices) of environment 300 may perform one or more functions described as being performed by another set of systems or another set of devices of environment 300.

[0109] Referring now to FIG. 4, shown is a diagram of example components of a device 900 according to non-limiting embodiments or aspects. Device 900 may correspond to at least one of access authorization system 102, server 104, user device 106, and/or data repository 108 in FIG. 1 and/or at least one of transaction service provider system 302, issuer system 304, customer device 306, merchant system 308, and/or acquirer system 310 in FIG. 3, as an example. In some non-limiting embodiments or aspects, such systems or devices in FIG. 1 or FIG. 3 may include at least one device 900 and/or at least one component of device 900. The number and arrangement of components shown in FIG. 4 are provided as an example. In some non-limiting embodiments or aspects, device 900 may include additional components, fewer components, different components, or differently arranged components than those shown in FIG. 4. Additionally, or alternatively, a set of components (e.g., one or more components) of device 900 may perform one or more functions described as being performed by another set of components of device 900.

[0110] As shown in FIG. 4, device 900 may include bus 902, processor 904, memory 906, storage component 908, input component 910, output component 912, and communication interface 914. Bus 902 may include a component that permits communication among the components of device 900. In some non-limiting embodiments, processor 904 may be implemented in hardware, firmware, or a combination of hardware and software. For example, processor 904 may include a processor (e.g., a central processing unit (CPU), a graphics processing unit (GPU), an accelerated processing unit (APU), etc.), a microprocessor, a digital signal processor (DSP), and/or any processing component (e.g., a field-programmable gate array (FPGA), an application-specific integrated circuit (ASIC), etc.) that can be programmed to perform a function. Memory 906 may include random access memory (RAM), read only memory (ROM), and/or another type of dynamic or static storage device (e.g., flash memory, magnetic memory, optical memory, etc.) that stores

information and/or instructions for use by processor 904. In some non-limiting embodiments or aspects, memory 906 may be the same as or similar to data repository 108.

[0111] With continued reference to FIG. 4, storage component 908 may store information and/or software related to the operation and use of device 900. For example, storage component 908 may include a hard disk (e.g., a magnetic disk, an optical disk, a magneto-optic disk, a solid state disk, etc.) and/or another type of computer-readable medium. In some non-limiting embodiments or aspects, storage component 908 may be the same as or similar to data repository 108. Input component 910 may include a component that permits device 900 to receive information, such as via user input (e.g., a touch screen display, a keyboard, a keypad, a mouse, a button, a switch, a microphone, etc.). Additionally, or alternatively, input component 910 may include a sensor for sensing information (e.g., a global positioning system (GPS) component, an accelerometer, a gyroscope, an actuator, etc.). Output component 912 may include a component that provides output information from device 900 (e.g., a display, a speaker, one or more light-emitting diodes (LEDs), etc.). Communication interface 914 may include a transceiver-like component (e.g., a transceiver, a separate receiver and transmitter, etc.) that enables device 900 to communicate with other devices, such as via a wired connection, a wireless connection, or a combination of wired and wireless connections. Communication interface 914 may permit device 900 to receive information from another device and/or provide information to another device. For example, communication interface 914 may include an Ethernet interface, an optical interface, a coaxial interface, an infrared interface, a radio frequency (RF) interface, a universal serial bus (USB) interface, a Wi-Fi® interface, a cellular network interface, and/or the like.

[0112] Device 900 may perform one or more processes described herein. Device 900 may perform these processes based on processor 904 executing software instructions stored by a computer-readable medium, such as memory 906 and/or storage component 908. A computer-readable medium may include any non-transitory memory device. A memory device includes memory space located inside of a single physical storage device or memory space spread across multiple physical storage devices. Software instructions may be read into memory 906 and/or storage component 908 from another computer-readable medium or from another device via communication interface 914. When executed, software instructions stored in memory

906 and/or storage component 908 may cause processor 904 to perform one or more processes described herein. Additionally, or alternatively, hardwired circuitry may be used in place of or in combination with software instructions to perform one or more processes described herein. Thus, embodiments described herein are not limited to any specific combination of hardware circuitry and software. The term "configured to," as used herein, may refer to an arrangement of software, device(s), and/or hardware for performing and/or enabling one or more functions (e.g., actions, processes, steps of a process, and/or the like). For example, "a processor configured to" may refer to a processor that executes software instructions (e.g., program code) that cause the processor to perform one or more functions.

[0113] Although embodiments have been described in detail for the purpose of illustration, it is to be understood that such detail is solely for that purpose and that the disclosure is not limited to the disclosed embodiments or aspects, but, on the contrary, is intended to cover modifications and equivalent arrangements that are within the spirit and scope of the appended claims. For example, it is to be understood that the present disclosure contemplates that, to the extent possible, one or more features of any embodiment or aspect can be combined with one or more features of any other embodiment or aspect.

WHAT IS CLAIMED IS:

1. A computer-implemented method comprising:

receiving, with at least one processor, an access request and data associated with a system record, the access request associated with a username of a user, the data associated with the system record comprising a change reason and a change identifier;

provisioning, with the at least one processor, ephemeral credentials to the user based on authenticating the user and based on the data associated with the system record;

authorizing, with the at least one processor, the user to access at least one target system associated with the access request based on the ephemeral credentials;

determining, with the at least one processor, that the user is no longer authorized to access the at least one target system based on the ephemeral credentials; and

terminating, with the at least one processor, access to the at least one target system based on determining that the user is no longer authorized to access a production server.

2. The computer-implemented method of claim 1, further comprising:

authenticating, with the at least one processor, the user using multifactor authentication based on the username of the user.

3. The computer-implemented method of claim 1, wherein the ephemeral credentials are based on a secure shell protocol.

4. The computer-implemented method of claim 1, further comprising:

prompting, with the at least one processor, the user to provide the data associated with the system record.

5. The computer-implemented method of claim 1, further comprising:

validating, with the at least one processor, the data associated with the system record with an initial system record stored in a data repository, wherein validating the data associated with the system record comprises:

determining that the data associated with the system record matches master data associated with the initial system record stored in the data repository; and

correlating the data associated with the system record with the username of the user based on the master data associated with the initial system record.

6. The computer-implemented method of claim 1, wherein provisioning the ephemeral credentials to the user comprises:

determining a duration of time associated with the system record based on the change reason; and

generating the ephemeral credentials comprising the duration of time associated with the system record, wherein the duration of time associated with the system record represents a time for which the ephemeral credentials are valid.

7. The computer-implemented method of claim 6, wherein determining that the user is no longer authorized to access the at least one target system comprises:

determining that the duration of time associated with the system record has lapsed.

8. The computer-implemented method of claim 1, wherein determining that the user is no longer authorized to access the at least one target system comprises:

detecting that the user has completed an action associated with the change reason and the change identifier.

9. The computer-implemented method of claim 1, wherein the ephemeral credentials comprise one or more user role accounts.

10. The computer-implemented method of claim 9, wherein authorizing the user to access the at least one target system comprises:

receiving a request for a connection from the user, the request comprising the ephemeral credentials;

determining that the one or more user role accounts of the ephemeral credentials is authorized to access the production server; and

initiating a communication session based on the one or more user role accounts, wherein the communication session is configured to transmit one or more messages between a user device of the user and the production server.

11. The computer-implemented method of claim 10, further comprising:

recording the communication session to generate a recorded communication session;

associating the recorded communication session with the username of the user that transmitted the request for the connection; and

storing the recorded communication session and the username of the user in a data repository.

12. The computer-implemented method of claim 10, wherein the communication session is based on a secure shell protocol.

13. The computer-implemented method of claim 1, wherein the ephemeral credentials comprise a key identifier, the key identifier comprising the username of the user and the change identifier.

14. The computer-implemented method of claim 13, further comprising:

logging, with the at least one processor, the key identifier, a time of authorization of the user, and a username of at least one user role account of the one or more user role accounts to a log record;

storing, with the at least one processor, the key identifier in cache memory of the at least one target system; and

retrieving, with the at least one processor, the username of the user of the key identifier from the cache memory of the production server based on a process identifier associated with the at least one target system.

15. The computer-implemented method of claim 13, wherein authorizing the user to access the at least one target system comprises:

receiving a request for a connection, the request comprising the ephemeral credentials;

retrieving master data associated with an initial system record stored in a data repository based on the change identifier of the key identifier matching a record identifier of the initial system record; and

correlating the at least one target system with the change reason based on an identifier associated with the at least one target system and a change reason of the master data associated with the initial system record.

16. The computer-implemented method of claim 15, wherein the data repository receives the master data in real-time from a configuration management database.

17. The computer-implemented method of claim 1, further comprising generating the ephemeral credentials by digitally signing a user key with a root private key.

18. The computer-implemented method of claim 17, further comprising:

generating the root private key and corresponding root public key in response to receiving a change request; and

distributing the root public key to a subset of production servers including the production server.

19. A system comprising:

at least one processor configured to:

receive an access request and data associated with a system record, the access request associated with a username of a user, the data

associated with the system record comprising a change reason and a change identifier;

provision ephemeral credentials to the user based on authenticating the user and based on the data associated with the system record;

authorize the user to access at least one target system associated with the access request based on the ephemeral credentials;

determine that the user is no longer authorized to access the at least one target system based on the ephemeral credentials; and

terminate access to the at least one target system based on determining that the user is no longer authorized to access a production server.

20. The system of claim 19, wherein the at least one processor is further configured to:

authenticate the user using multifactor authentication based on the username of the user.

21. The system of claim 19, wherein the ephemeral credentials are based on a secure shell protocol.

22. The system of claim 19, wherein the at least one processor is further configured to:

prompt the user to provide the data associated with the system record.

23. The system of claim 19, wherein the at least one processor is further configured to:

validate the data associated with the system record with an initial system record stored in a data repository, wherein validating the data associated with the system record comprises:

determining that the data associated with the system record matches master data associated with the initial system record stored in the data repository; and

correlating the data associated with the system record with the username of the user based on the master data associated with the initial system record.

24. The system of claim 19, wherein provisioning the ephemeral credentials to the user comprises:

determining a duration of time associated with the system record based on the change reason; and

generating the ephemeral credentials comprising the duration of time associated with the system record, wherein the duration of time associated with the system record represents a time for which the ephemeral credentials are valid.

25. The system of claim 24, wherein determining that the user is no longer authorized to access the at least one target system comprises:

determining that the duration of time associated with the system record has lapsed.

26. The system of claim 19, wherein determining that the user is no longer authorized to access the at least one target system comprises:

detecting that the user has completed an action associated with the change reason and the change identifier.

27. The system of claim 19, wherein the ephemeral credentials comprise one or more user role accounts.

28. The system of claim 27, wherein authorizing the user to access the at least one target system comprises:

receiving a request for a connection from the user, the request comprising the ephemeral credentials;

determining that the one or more user role accounts of the ephemeral credentials is authorized to access the production server; and

initiating a communication session based on the one or more user role accounts, wherein the communication session is configured to transmit one or more messages between a user device of the user and the production server.

29. The system of claim 28, wherein the at least one processor is further configured to:

record the communication session to generate a recorded communication session;

associate the recorded communication session with the username of the user that transmitted the request for the connection; and

store the recorded communication session and the username of the user in a data repository.

30. The system of claim 28, wherein the communication session is based on a secure shell protocol.

31. The system of claim 19, wherein the ephemeral credentials comprise a key identifier, the key identifier comprising the username of the user and the change identifier.

32. The system of claim 31, wherein the at least one processor is further configured to:

log the key identifier, a time of authorization of the user, and a username of at least one user role account of the one or more user role accounts to a log record;

store the key identifier in cache memory of the at least one target system; and

retrieve the username of the user of the key identifier from the cache memory of the production server based on a process identifier associated with the at least one target system.

33. The system of claim 31, wherein authorizing the user to access the at least one target system comprises:

receiving a request for a connection, the request comprising the ephemeral credentials;

retrieving master data associated with an initial system record stored in a data repository based on the change identifier of the key identifier matching a record identifier of the initial system record; and

correlating the at least one target system with the change reason based on an identifier associated with the at least one target system and a change reason of the master data associated with the initial system record.

34. The system of claim 33, wherein the data repository receives the master data in real-time from a configuration management database.

35. The system of claim 19, wherein the at least one processor is further configured to generating the ephemeral credentials by digitally signing a user key with a root private key.

36. The system of claim 35, wherein the at least one processor is further configured to:

generate the root private key and corresponding root public key in response to receiving a change request; and

distribute the root public key to a subset of production servers including the production server.

37. A computer program product comprising at least one non-transitory computer-readable medium including program instructions that, when executed by at least one processor, cause the at least one processor to:

receive an access request and data associated with a system record, the access request associated with a username of a user, the data associated with the system record comprising a change reason and a change identifier;

provision ephemeral credentials to the user based on authenticating the user and based on the data associated with the system record;

authorize the user to access at least one target system associated with the access request based on the ephemeral credentials;

determine that the user is no longer authorized to access the at least one target system based on the ephemeral credentials; and

terminate access to the at least one target system based on determining that the user is no longer authorized to access a production server.

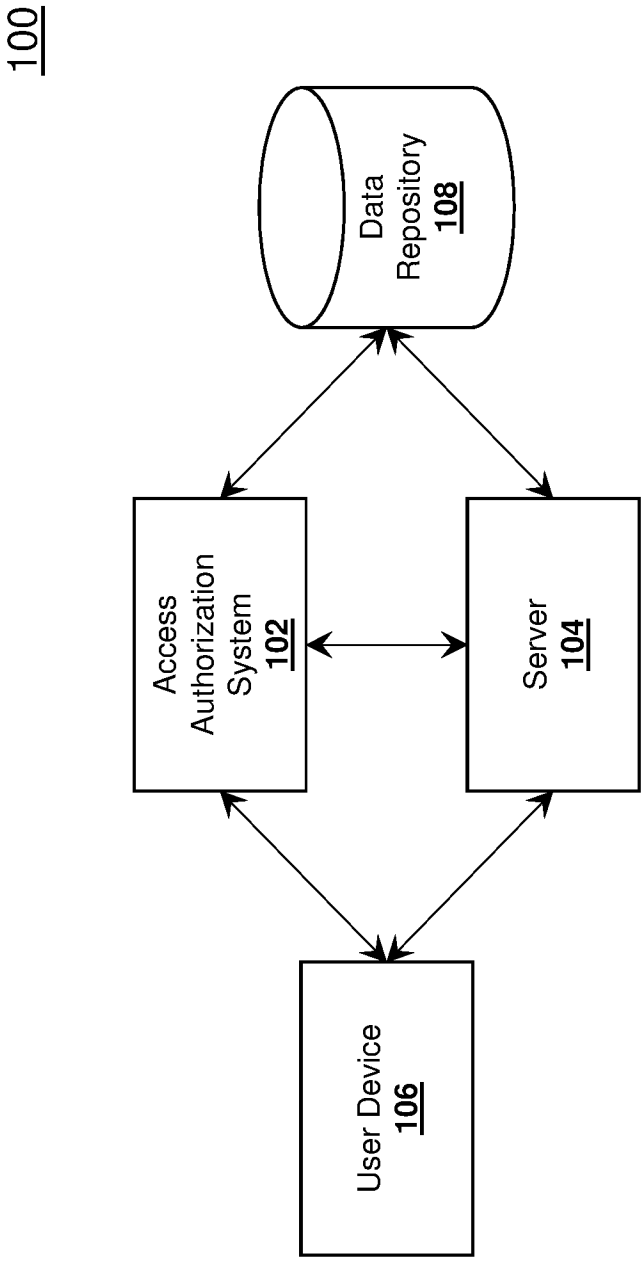
100
Data Repository 108
Access Authorization System 102
Server 104
User Device 106

FIG. 1

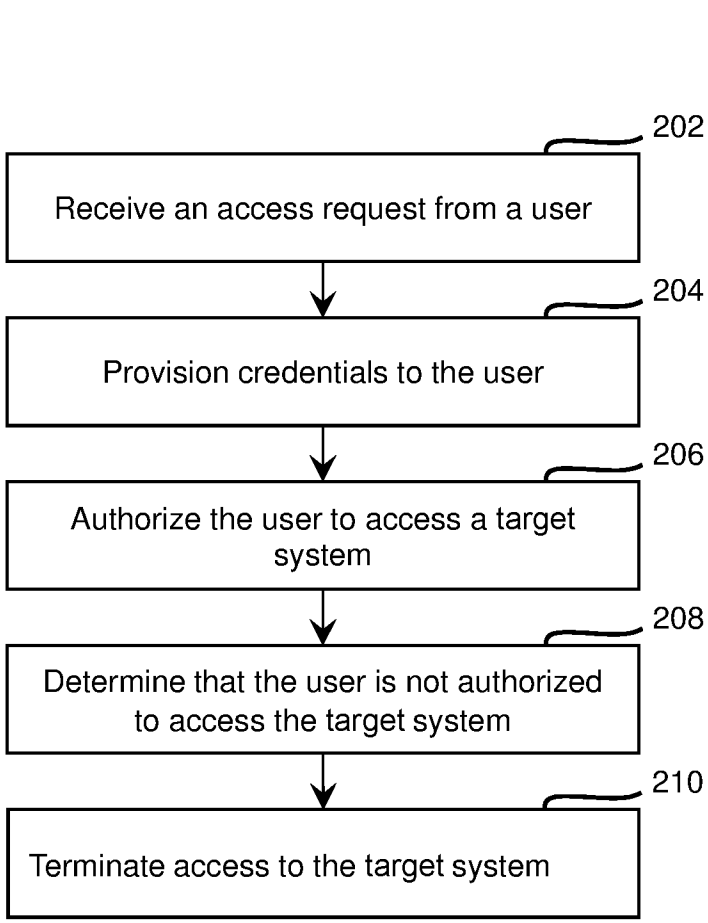
200
202
Receive an access request from a user
204
Provision credentials to the user
206
Authorize the user to access a target system
208
Determine that the user is not authorized to access the target system
210
Terminate access to the target system

FIG. 2

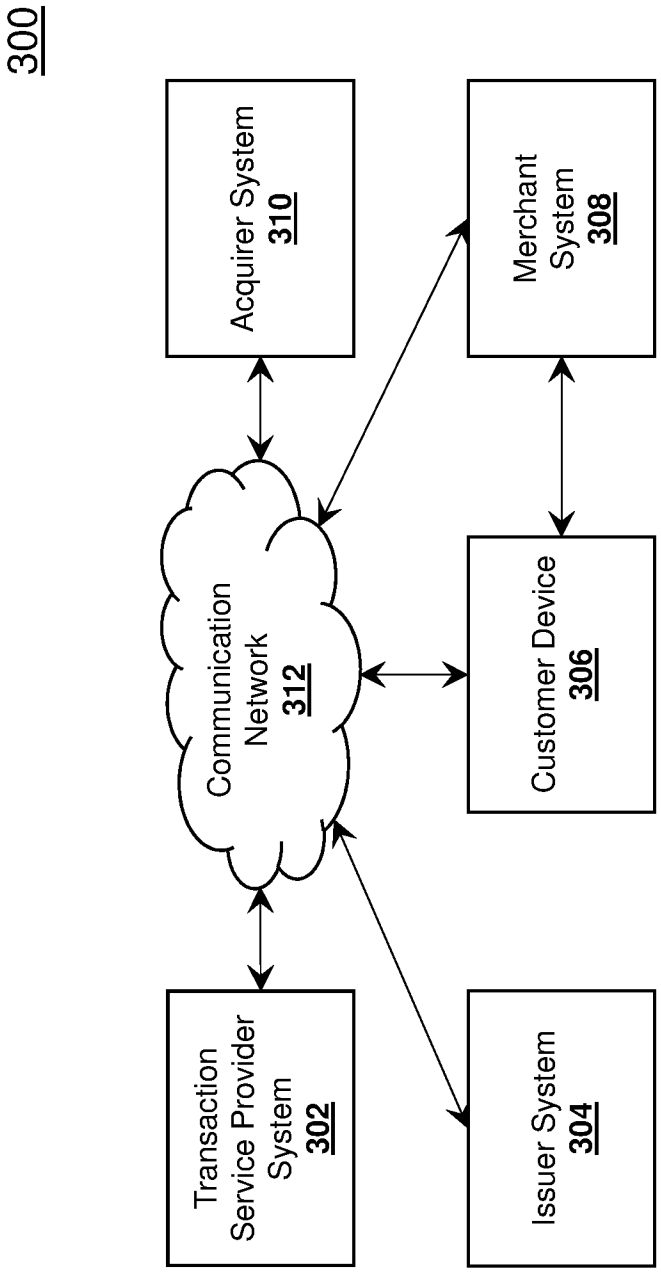
300
Acquirer System
310
Merchant
System
308
Communication
Network
312
Customer Device
306
Transaction
Service Provider
System
302
Issuer System
304

FIG. 3

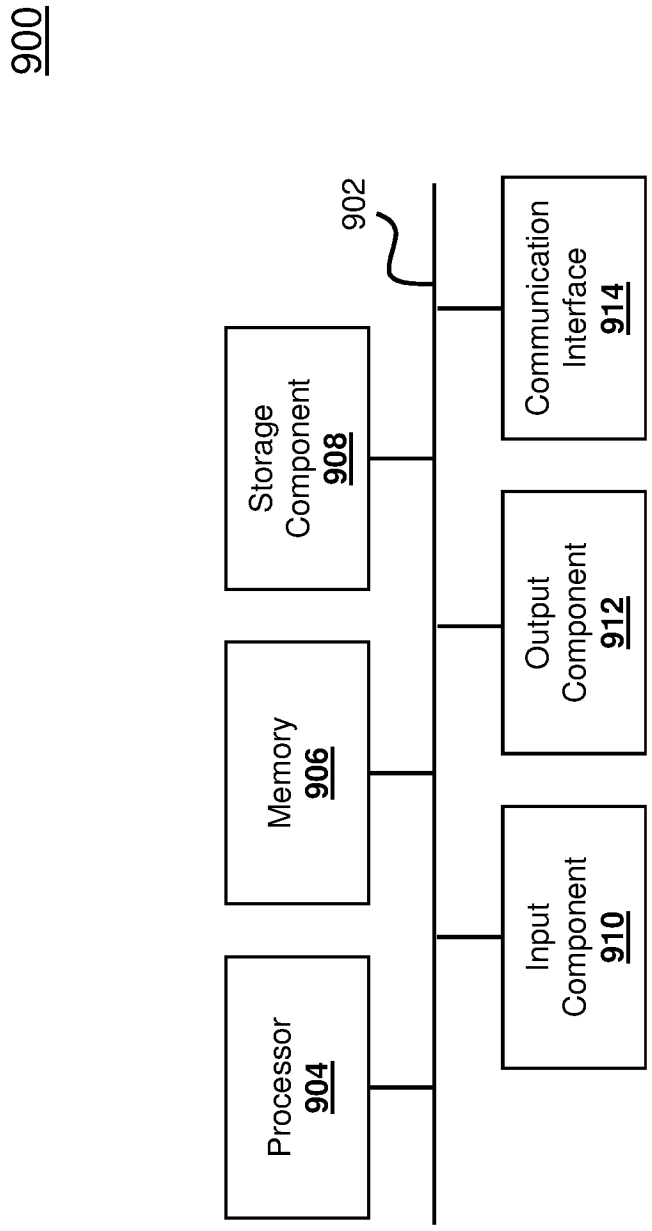
900
902
Processor 904
Memory 906
Storage Component 908
Input Component 910
Output Component 912
Communication Interface 914

FIG. 4