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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 February 2025 (27.02.2025)

WIPO | PCT

(10) International Publication Number
WO 2025/042652 A2

(51) International Patent Classification:
H04L 9/32 (2006.01) *G06Q 10/10* (2023.01)

(21) International Application Number:
PCT/US2024/042269

(22) International Filing Date:
14 August 2024 (14.08.2024)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
63/533,410 18 August 2023 (18.08.2023) US

(71) Applicant: **GOVERNMENT OF THE UNITED STATES OF AMERICA, AS REPRESENTED BY THE SECRETARY OF COMMERCE** [US/US]; National Institute of Standards and Technology, 100 Bureau Drive, MS 1052, Gaithersburg, Maryland 20899 (US).

(72) Inventors: **BARNARD FEENEY, Allison**; National Institute of Standards and Technology, 100 Bureau Drive, MS 1052, Gaithersburg, Maryland 20899 (US). **KRIMA, Sylvere Ismael**; National Institute of Standards and Technology, 100 Bureau Drive, MS 1052, Gaithersburg, Maryland 20899 (US).

(74) Agent: **NAIR, Rajesh B.**; National Institute of Standards and Technology, 100 Bureau Drive, MS 1052, Gaithersburg, Maryland 20899 (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,

(54) Title: SYSTEM AND METHOD FOR MANAGING ENGINEERING CERTIFICATES

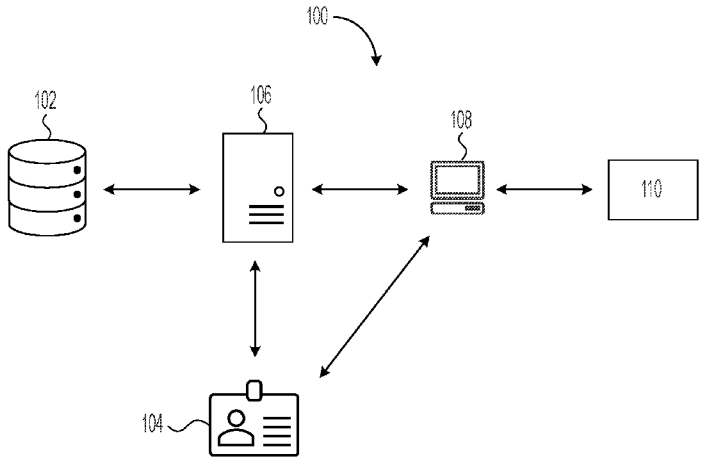

FIG. 1

(57) Abstract: Embodiments of the present invention relate to systems and methods for managing trustworthy engineering certificates. More particularly, embodiments of the present invention relate to systems and methods for signing, validating, and auditing technical certificates, such as manufacturing and engineering certificates. Engineering certificate management systems in accordance with embodiments of the present invention includes an information system for the storage and retrieval of all data produced and required for the operation of engineering certification system, an identity provider, a server, a client interface, and a cyber-physical device. Trustworthy engineering certificates management methods in accordance with embodiments of the present invention includes the steps of managing accounts, authentication, accounts activation, configuring engineering certificates, issuing engineering certificates, and retrieving certificates.

WO 2025/042652 A2

[Continued on next page]

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.

(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).

Published:

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

SYSTEM AND METHOD FOR MANAGING ENGINEERING CERTIFICATES

CROSS-REFERENCE TO RELATED APPLICATION

This application claims the benefit of priority from U.S. Provisional Patent Application Ser. No. 63/533,410, filed on August 18, 2023, the disclosure of which is incorporated herein by reference in its entirety.

STATEMENT REGARDING FEDERAL RIGHTS

The invention described herein was made with United States Government support from the National Institute of Standards and Technology (NIST), an agency of the United States Department of Commerce. The United States Government has certain rights in the invention.

FIELD OF THE INVENTION

The present invention relates generally to digital data security, and more particularly, to issuing and validating engineering certificates in a trusted environment.

BACKGROUND OF THE INVENTION

Digital product data is key to most manufacturers' operations, including small-to-medium-size manufacturers. Part of that data includes authentication and authorization metadata, also known as engineering certification. Manufacturers rely on that metadata and its integrity to make decisions about the right data to use in their operations. Before digitalization, the integrity and validity of those certificates depended on recognized physical signatures from trusted authorities. Accordingly, there is a need for a mechanism for managing trustworthy engineering certificates in the digital world, which achieves by leveraging digital signatures, blockchain technology, and allowing software and human users to issue and validate engineering certificates in a trusted environment.

SUMMARY OF THE INVENTION

Embodiments of the present invention relate to systems and methods for managing trustworthy engineering certificates. More particularly, embodiments of the present invention relate to systems and methods for signing, validating, and auditing technical certificates, such as manufacturing and

engineering certificates. Systems and methods in accordance with embodiments of the present invention for managing trustworthy engineering certificates include a novel combination of multiple characteristics: 1) signed certificates that are not embedded but detached from the technical data, represented in a standardized format (JSON Web Signature and JSON Web Token), and stored in a central repository, thereby simplifying their auditing; 2) a repository leveraging a verifiable and auditable centralized blockchain-based digital ledger to protect and demonstrate the integrity of the certificates without the overhead of a distributed ledger; 3) providing users full control of their private key used to digitally sign the technical data, while the keys are securely stored in a central repository using a secure remote password protocol, thereby simplifying their management, 4) enabling users to create and reuse customized technical certificate templates based on their company's product data workflow requirements, thereby reducing duplicate and manual efforts required to issue and sign certificates, 5) enabling users to organize certificates and certificate templates by workspaces to create or replicate organizational structures such as business units or projects; 6) enabling automated validation of certificates; and 7) exposing all features through an API to integrate with existing tools or new ones, thereby enabling automation.

Embodiments of the present invention relate to a computer-implemented method for managing a plurality of engineering certificates, said method including determining whether an identity provider is a gateway to a plurality of first credentials; providing a plurality of second credentials for a plurality of users, wherein the identity provider is not the gateway to the plurality of the first credentials; authorizing access to an account for at least one of the plurality of the users using the plurality of the second credentials, wherein the authorizing the access to the account for the at least one of the plurality of the users includes: providing from the identity provider to the at least one of the plurality of the users an authentication challenge; receiving by the identity provider from the at least one of the plurality of the users a third credential in response to the authentication challenge; and validating by the identity provider the third credential received from the at least one of the plurality of the users; activating the account for the validated at least one of the plurality of the users, wherein the activating the account for the validated at least one of the plurality of the users includes: generating an encrypted private key for the validated at least one of the plurality of the users; associating the encrypted private key to the validated at least one of the plurality of the users; and storing in an information system the associated encrypted private key for the validated at least one of the plurality of the users; generating a first certificate profile for the validated at

least one of the plurality of the users, wherein the generating the first certificate profile comprises recording and encoding a second certificate profile received from the at least one of the plurality of the users; storing the generated first certificate profile in the information system; applying a predetermined algorithm to generate a first identifier for an engineering artifact; generating the at least one of the plurality of the engineering certificates from the second certificate profile and the engineering artifact; retrieving from the information system the associated encrypted private key for the validated at least one of the plurality of the users; and issuing a payload comprising the generated engineering certificate, the first identifier for the engineering artifact and the applied predetermined algorithm for the generating the first identifier for the engineering artifact, wherein the issuing the payload includes: receiving from a server the encrypted private key for the at least one of the plurality of the users; decrypting the encrypted private key for the at least one of the plurality of the users, wherein the decrypting the encrypted private key generates a decrypted private key; signing the payload for the engineering artifact using the decrypted private key; validating the signed payload for the engineering artifact; associating the signed payload for the engineering artifact with a public key for the at least one of the plurality of the users; storing the signed payload for the engineering artifact and the associated public key in the information system; and generating an operational status indicating the signed payload for the engineering artifact. More particularly, the third credential is a username and password or a token.

In one embodiment of the present invention, the computer-implemented method for managing a plurality of engineering certificates further includes retrieving the at least one of the plurality of the issued engineering certificates, wherein the retrieving the at least one of the plurality of the issued engineering certificates includes: receiving the first identifier for the engineering artifact for the at least one of the plurality of the users; querying the information system for the signed engineering certificate using the first identifier for the engineering artifact and for the stored public key associated with the signed engineering certificate; retrieving the signed engineering certificates and the stored public key associated with the signed engineering certificate; and validating the retrieved signed engineering certificate using the stored public key associated with the signed engineering certificate.

In some embodiments of the present invention, the identity provider generates a second identifier for the validated at least one of the plurality of the users, wherein the storing in the information

system the associated the encrypted private key for the validated at least one of the plurality of the users includes: generating a third identifier for the validated at least one of the plurality of the users; associating the third identifier for the validated at least one of the plurality of the users with the second identifier generated by the identity provider for the validated at least one of the plurality of the users; and storing in the information system the third identifier for the validated at least one of the plurality of the users with the second identifier generated by the identity provider for the validated at least one of the plurality of the users.

Another embodiment of the present invention relates to a system for managing engineering certificates, including one or more processors; and one or more non-transitory computer-readable storage mediums in communication with the one or more processing systems and encoded with instructions for commanding the one or more processing systems to execute steps including: determining whether an identity provider is a gateway to a plurality of first credentials; providing a plurality of second credentials for a plurality of users, wherein the identity provider is not the gateway to the plurality of the first credentials; authorizing access to an account for at least one of the plurality of the users using the plurality of the second credentials, wherein the authorizing the access to the account for the at least one of the plurality of the users includes: providing from the identity provider to the at least one of the plurality of the users an authentication challenge; receiving by the identity provider from the at least one of the plurality of the users a third credential in response to the authentication challenge; and validating by the identity provider the third credential received from the at least one of the plurality of the users; activating the account for the validated at least one of the plurality of the users, wherein the activating the account for the validated at least one of the plurality of the users includes: generating an encrypted private key for the validated at least one of the plurality of the users; associating the encrypted private key to the validated at least one of the plurality of the users; and storing in an information system the associated encrypted private key for the validated at least one of the plurality of the users; generating a first certificate profile for the validated at least one of the plurality of the users, wherein the generating the first certificate profile comprises recording and encoding a second certificate profile received from the at least one of the plurality of the users; storing the generated first certificate profile in the information system; applying a predetermined algorithm to generate a first identifier for an engineering artifact; generating the at least one of the plurality of the engineering certificates from the second certificate profile and the engineering artifact; retrieving

from the information system the associated encrypted private key for the validated at least one of the plurality of the users; and issuing a payload comprising the generated engineering certificate, the first identifier for the engineering artifact and the applied predetermined algorithm for the generating the first identifier for the engineering artifact, wherein the issuing the payload includes: receiving from a server the encrypted private key for the at least one of the plurality of the users; decrypting the encrypted private key for the at least one of the plurality of the users, wherein the decrypting the encrypted private key generates a decrypted private key; signing the payload for the engineering artifact using the decrypted private key; validating the signed payload for the engineering artifact; associating the signed payload for the engineering artifact with a public key for the at least one of the plurality of the users; storing the signed payload for the engineering artifact and the associated public key in the information system; and generating an operational status indicating the signed payload for the engineering artifact. More particularly, the third credential is a username and password or a token.

In one embodiments of the present invention, the instructions for commanding the one or more processing systems to execute steps further comprises retrieving the at least one of the plurality of the issued engineering certificates, wherein the retrieving the at least one of the plurality of the issued engineering certificates includes: receiving the first identifier for the engineering artifact for the at least one of the plurality of the users; querying the information system for the signed engineering certificate using the first identifier for the engineering artifact and for the stored public key associated with the signed engineering certificate; retrieving the signed engineering certificates and the stored public key associated with the signed engineering certificate; and validating the retrieved signed engineering certificate using the stored public key associated with the signed engineering certificate.

Embodiments of the present invention also relate to a non-transitory computer-readable medium storing a program causing a computer to execute a method for managing engineering certificates, the method including: determining whether an identity provider is a gateway to a plurality of first credentials; providing a plurality of second credentials for a plurality of users, wherein the identity provider is not the gateway to the plurality of the first credentials; authorizing access to an account for at least one of the plurality of the users using the plurality of the second credentials, wherein the authorizing the access to the account for the at least one of the plurality of the users includes:

providing from the identity provider to the at least one of the plurality of the users an authentication challenge; receiving by the identity provider from the at least one of the plurality of the users a third credential in response to the authentication challenge; and validating by the identity provider the third credential received from the at least one of the plurality of the users; activating the account for the validated at least one of the plurality of the users, wherein the activating the account for the validated at least one of the plurality of the users includes: generating an encrypted private key for the validated at least one of the plurality of the users; associating the encrypted private key to the validated at least one of the plurality of the users; and storing in an information system the associated encrypted private key for the validated at least one of the plurality of the users; generating a first certificate profile for the validated at least one of the plurality of the users, wherein the generating the first certificate profile comprises recording and encoding a second certificate profile received from the at least one of the plurality of the users; storing the generated first certificate profile in the information system; applying a predetermined algorithm to generate a first identifier for an engineering artifact; generating the at least one of the plurality of the engineering certificates from the second certificate profile and the engineering artifact; retrieving from the information system the associated encrypted private key for the validated at least one of the plurality of the users; and issuing a payload comprising the generated engineering certificate, the first identifier for the engineering artifact and the applied predetermined algorithm for the generating the first identifier for the engineering artifact, wherein the issuing the payload includes: receiving from a server the encrypted private key for the at least one of the plurality of the users; decrypting the encrypted private key for the at least one of the plurality of the users, wherein the decrypting the encrypted private key generates a decrypted private key; signing the payload for the engineering artifact using the decrypted private key; validating the signed payload for the engineering artifact; associating the signed payload for the engineering artifact with a public key for the at least one of the plurality of the users; storing the signed payload for the engineering artifact and the associated public key in the information system; and generating an operational status indicating the signed payload for the engineering artifact.

In one embodiment of the present invention, the non-transitory computer-readable medium storing a program causing a computer to execute a method for managing engineering certificates further includes retrieving the at least one of the plurality of the issued engineering certificates, wherein the retrieving the at least one of the plurality of the issued engineering certificates includes:

receiving the first identifier for the engineering artifact for the at least one of the plurality of the users; querying the information system for the signed engineering certificate using the first identifier for the engineering artifact and for the stored public key associated with the signed engineering certificate; retrieving the signed engineering certificates and the stored public key associated with the signed engineering certificate; and validating the retrieved signed engineering certificate using the stored public key associated with the signed engineering certificate.

BRIEF DESCRIPTION OF DRAWINGS

FIG. 1 illustrates a system for managing trustworthy engineering certificates in accordance with embodiments of the present invention.

FIG. 2 illustrates a flow chart for a method for managing trustworthy engineering certificates.

FIG. 3 illustrates a schematic representation of a method for activating accounts in accordance with embodiments of the present invention.

FIG. 4 illustrates a schematic representation of a method for configuring engineering certificates in accordance with embodiments of the present invention.

FIG. 5 illustrates a schematic representation of a method for issuing engineering certificates in accordance with embodiments of the present invention.

FIG. 6 illustrates a schematic representation of a method for retrieving certificates in accordance with embodiments of the present invention.

DETAILED DESCRIPTION

While the making and using of various embodiments of the present invention are discussed in detail below, it should be appreciated that the present invention provides many applicable inventive concepts which can be embodied in a wide variety of specific contexts. The specific embodiments discussed herein are merely illustrative of specific ways to make and use the invention, and do not delimit the scope of the present invention. Reference will now be made to the drawings wherein like numerals refer to like elements throughout.

Referring now to the drawings, and more particularly, to FIG. 1, there is shown a trustworthy engineering certification system, generally designated **100** and schematically showing an embodiment of the present invention, for managing trustworthy engineering certificates. Engineering certificate management system **100** includes an information system **102** for the storage and retrieval of all data produced and required for the operation of engineering certification system **100**, an identity provider **104**, a server **106**, a client interface **108**, and a cyber-physical device **110**.

Information system **102** allows for the storage and retrieval of all data produced and required for the operation of engineering certification system **100**. Information system **102** can be implemented using a database of any type (e.g., relational, document, or graph) or any other solution that supports a controlled access mechanism (e.g., protected by a password). Identity provider **104** manages identities and credentials or acts as a gateway to other and existing providers in use and functions as a trusted source of user identities and credentials. Server **106** allows for implementing methods in accordance with embodiments of the present invention, for providing an authentication and authorization mechanism, and for exposing methods in accordance with embodiments of the present invention to a client system through an Application Programming Interface such as a library, Remote API, or Web API. Client **108** provides an interface between a user and server **106** using identity provider **104**. Information system **102**, identity provider **104**, server **106** and client **108** can be configured, operated and maintained by an administrator having appropriate authorization to perform such functions. Cyber-physical system **110** allows an entity to issue, retrieve, and validate engineering certificates.

FIG. 2 illustrates a flow chart for a method for managing trustworthy engineering certificates **200**. Trustworthy engineering certificates management method **200** includes the steps of managing accounts **202**, authentication **204**, accounts activation **206**, configuring engineering certificates **208**, issuing engineering certificates **210**, and retrieving certificates **212**. Managing accounts **202** includes determining whether identity provider **104** is a gateway to an existing source of identities and credentials, and using identity provider **104** to provision identities and credentials for users when identity provider **104** is not a gateway to an existing source of identities and credentials. Selected user identities and credentials are authorized to issue and retrieve engineering certificates. Authentication **204** includes accessing identity provider **104** through client **108** and completing an

authentication challenge to authorize access to a user account. Exemplary response to authentication challenges includes providing username and password, token, biometrics, and the like. Authentication **204** step determines whether the user has successfully completed the challenge and request's identity provider **104** to send back a proof of successful authentication if the user has successfully completed the challenge, which client **108** will attach to every single user request to server **106**. Server **106** validates the proof of successful authentication with identity provider **104** for each request.

FIG. 3 illustrates a method for a user account activation **206** in accordance with embodiments of the present invention before the user can use client **108** to issue or retrieve an engineering certificate. First, the user must authenticate itself through client **108** and identity provider **104**. At operational step **302**, client **108** receives a request for access to an account and submits the request for access to an account to identity provider **104**. At operational step **304**, identity provider **104** issues a challenge, receives an attempt at the challenge from user at step **306** and, at step **308**, identity provider **104** verifies the challenge attempt received from the user. Account activation **206** method determines, at step **310**, whether the challenge attempt verification at step **308** is successful and, if successful, client **108** then generates a private key at step **312** and encrypts the private key at step **316** with an encryption key input received from the user at step **314**. This encrypted private key, its corresponding public key, and any decryption parameter (other than the decryption key) are sent to server **106** and, at step **318**, stored in information system **102** in a manner that associates the encrypted private key to the user and in a manner that allows retrieval using the user's unique identifiers. During this step, server **106** creates a local unique identifier for the user and stores it in information system **102** in association with the user's identity provider identifier. Server **106** generates an activation status at step **318** for client **108** and, at step **322**, client **108** then prepares a status message for display to user.

FIG. 4 illustrates a method for configuring engineering certificates **208** in accordance with embodiments of the present invention to facilitate reuse and enforce consistency across users, and validate engineering certificates, at server **106** and client **108** such that authenticated users at authentication **204** step can define, store, and retrieve certificate templates or models. At operational step **402**, client **108** receives a certificate profile from the user and, at step **404**, client **108** creates a digital certificate profile by recording and encoding the profile received from the

user. In one embodiment of the present invention, a template or profile is a list of required typed data fields to be populated by the user and included in the certificate. By using templates, users can populate the same data fields and provide consistent information to consumers of those certificates. The digital profile created at step **404** is sent to server **106** and, at step **406**, server **106** stores the digital profile in information system **102**. At step **408**, client **108** generates a notification that the digital profile is recorded and provides the notification to the user.

FIG. 5 illustrates a method for issuing engineering certificates **210** in accordance with embodiments of the present invention to enable a user to create and sign an engineering certificate related to a digital engineering artifact once their account has been activated. Issuing engineering certificates **210** step requires an authenticated user, through client **108** to: i) pick a method to generate a reproducible and unique identifier from the engineering artifact; ii) use such method to generate the unique identifier; iii) provide a digital version of the engineering certificate generated using the engineering artifact and the certificate profile received from the user; iv) retrieve their encrypted private key and decryption parameters; v) decrypt their encrypted private key using the decryption parameters and their decryption key; vi) use the decrypted private key to digitally sign and validate a payload of the artifact unique identifier, the name of the method used to generate this identifier, and a copy of the digital engineering certificate; and vii) send the digitally signed payload and any additional data required by the server for storage. Issuing engineering certificates method **210** receives a request to prepare a payload for an engineering artifact at operational step **502**. At operational step **504**, client **108** generates a unique artifact identifier and requests an encrypted private key from the user at step **506**. Upon receiving the payload, issuing engineering certificates **210** step requires server **106** to: i) retrieve the user's public key; ii) use that key and other data to validate the signature and stop any processing if the validation fails; and iii) store the payload and additional data in the information system such that the data can be retrieved using at least the artifact unique identifier. A request for the encrypted private key is issued from the user at step **506** and server **106** retrieves the key from information system **102** at step **508**. At step **510**, client **108** requests user to provide a decryption key and receives the decryption key at step **512**. At step **514**, the encrypted private key is decrypted using the decryption key received at step **512**. At decision step **516**, issuing engineering certificates method **210** determines whether the decryption is successful. If the decryption is unsuccessful, then client **108** requests user to provide another decryption key at step **510**. If the decryption is successful, then the payload is signed at

step **518** and the signature is verified by server **106** at step **520**. At decision step **522**, server **106** determines whether the signature verification at step **520** is successful. If signature verification at step **520** is successful, then, at step **524**, server **106** associates the signed payload for the engineering artifact with the public key for the user and stores the associated public key and the signed payload in information system **102**. At operational step **526**, client **108** generates an operational status including the signed payload and provides the status to the user.

FIG. 6 illustrates a method in accordance with embodiments of the present invention for retrieving certificates **212** through client **108**. Retrieving certificates **212** process receives, at step **602**, one or more artifact unique identifier or other additional data as search parameters for submission to server **106**. At operational step **604**, client **108** sends these criteria to server **106**, which uses the criteria to query information system **102** at step **606**, and returns any matching signed engineering certificates at step **610** with corresponding validation public key (step **608**) to client **108** for communication to the user. At step **612**, retrieving certificates **212** process requests client **108** to validate every single result using the corresponding validation public key and is provided to the user for evaluation at step **614**. Retrieving certificates **212** process permits client **108** to share all validation data to the user to allow them to run their validation independently.

Reference to the specific examples which follow and included herein are intended to provide a clearer understanding of systems and methods in accordance with embodiments of the present invention. The examples should not be construed as a limitation upon the scope of the present invention. The following examples describe strawman use cases for an engineering and manufacturing facility (Production Agency) that develops advanced solutions for complex systems, from prototype simulations to production to quality testing.

EXAMPLE 1. Use Case 1 – Design Authorization, Acceptance

Roles

Production Agency	Artifact – e.g., a model, a Technical Data Package
Program	Author
Design Agency	Lead

Scenario

The Production Agency partners with other organizations on Programs. Production Agency and its Design Agency have a Trust Model wherein Artifacts are certified through given protocols and guaranteed to meet quality expectations. If an Artifact is authorized for release by a Design Agency, Production Agency can trust that the Artifact can be used for that purpose. When Production Agency receives the Artifact they can authenticate certification and authorization of the Artifact.

This Design Agency has 1000 data Authors. Each Author can notify their Lead (one of 80) that they are finished authoring the Artifact and request that the Lead certify the quality of the Artifact according to the shared Trust Model. Once completed and all issues resolved, the Lead creates a certificate within EasyTrust, populating the Design Authorization metadata profile (see Fig. 1) with required evidence of certification. The Lead selects the Artifact, digitally signs the certificate and transmits the Artifact to Production Agency.

Upon receipt, Production Agency will receive the Artifact, retrieve its certificates in EasyTrust, validate their authenticity, then copy the authenticated Artifact into their PDM system for configuration management.

EXAMPLE 2. Use Case 2 – Process Engineer Supplier

Roles

Production Agency	Project Engineer
Program	Process Engineer
Design Agency	Supplier

Scenario

Production Agency assigns an authenticated design Artifact stored in their PDM system to a Project Engineer. The Project Engineer opens EasyTrust and validates the Artifact based in the certificates and their authenticity. If the Artifact has appropriate certificates according to rules for Design Authorization, and is valid, the Project Engineer begins work on the Artifact. Changes to the Artifact are saved and managed in the PDM system.

In this case, the Project Engineer notes a manufacturing requirement that necessitates involvement of a Process Engineer and forwards the Artifact to a Process Engineer.

The Process Engineer makes changes to the Artifact, which are logged in the PDM system. The Process Engineer creates a certificate for the Process Authorization and returns the altered Artifact to the Project Engineer.

At this point, the Project Engineer validates the Artifact, reviews it and determines that the Artifact will be manufactured externally. The Project Engineer selects a Supplier, creates a certificate for the Engineering Authorization, and sends the Artifact to the Supplier.

EXAMPLE 3. Use Case 3 - Design Artifact has Improper Meta-Data for Design Authorization.

Roles

Production Agency	Artifact
Program	Project Engineer

Scenario

Production Agency receives a product design from a Design Agency for fabrication. Production Agency validates the Artifact and learns that the Artifact is unchanged and is from the Design Agency as expected. A Project Engineer is assigned to work on the Artifact. The Project Engineer examines the Design Authorization certificate data for correctness and completeness and finds that the data does not satisfy the rules for the Design Authorization. Production Agency returns the artifact to the Design Agency and asks for the artifact to be re-certified.

Trustworthy engineering certificate management systems and methods in accordance with embodiments of the present invention have several advantages over previous certificate management systems and methods. Organizations rely on these engineering certificates and their integrity to make decisions about the right data to use in their operations. Before digitalization, the integrity and validity of those certificates depended on recognized physical signatures from trusted authorities. Trustworthy engineering certificate management systems and methods in accordance with embodiments of the present invention enable secure and verifiable creation, storage, exchange, and consumption of engineering certificates. Unlike more traditional solutions, trustworthy engineering certificate management systems and methods in accordance with embodiments of the present invention does not require a certificate authority or public key certificates, and reduces complexity and cost of deployment, maintenance, and operation of the

systems and methods. Systems and methods in accordance with embodiments of the present invention for managing trustworthy engineering certificates include a novel combination of multiple characteristics: 1) signed certificates that are not embedded but detached from the technical data, represented in a standardized format (JSON Web Signature and JSON Web Token), and stored in a central repository, thereby simplifying their auditing; 2) a repository leveraging a verifiable and auditable centralized blockchain-based digital ledger to protect and demonstrate the integrity of the certificates without the overhead of a distributed ledger; 3) providing users full control of their private key used to digitally signed the technical data, while the keys are securely stored in a central repository using a secure remote password protocol, thereby simplifying their management, 4) enabling users to create and reuse customized technical certificate templates based on their company's product data workflow requirements, thereby reducing duplicate and manual efforts required to issue and sign certificates, 5) enabling users to organize certificates and certificate templates by workspaces to create or replicate organizational structures such as business units or projects; and 6) exposing all features are exposed through an API to integrate with existing tools or new ones, thereby enabling automation.

Trustworthy engineering certificate management systems and methods in accordance with one or more embodiments of the present invention can be adapted to a variety of configurations. It is thought that trustworthy engineering certificate management system and methods in accordance with various embodiments of the present invention and many of its attendant advantages will be understood from the foregoing description and it will be apparent that various changes may be made without departing from the spirit and scope of the invention or sacrificing all of its material advantages, the form hereinbefore described being merely a preferred or exemplary embodiment thereof.

Those familiar with the art will understand that embodiments of the invention may be employed, for various specific purposes, without departing from the essential substance thereof. The description of any one embodiment given above is intended to illustrate an example rather than to limit the invention. This above description is not intended to indicate that any one embodiment is necessarily preferred over any other one for all purposes, or to limit the scope of the invention by describing any such embodiment, which invention scope is intended to be determined by the

claims, properly construed, including all subject matter encompassed by the doctrine of equivalents as properly applied to the claims.

CLAIMS

What is claimed is:

1. A computer-implemented method for managing a plurality of engineering certificates, said method comprising:

determining whether an identity provider is a gateway to a plurality of first credentials;

providing a plurality of second credentials for a plurality of users, wherein the identity provider is not the gateway to the plurality of the first credentials;

authorizing access to an account for at least one of the plurality of the users using the plurality of the second credentials, wherein the authorizing the access to the account for the at least one of the plurality of the users comprises:

providing from the identity provider to the at least one of the plurality of the users an authentication challenge;

receiving by the identity provider from the at least one of the plurality of the users a third credential in response to the authentication challenge; and

validating by the identity provider the third credential received from the at least one of the plurality of the users;

activating the account for the validated at least one of the plurality of the users, wherein the activating the account for the validated at least one of the plurality of the users comprises:

generating an encrypted private key for the validated at least one of the plurality of the users;

associating the encrypted private key to the validated at least one of the plurality of the users; and

storing in an information system the associated encrypted private key for the validated at least one of the plurality of the users;

generating a first certificate profile for the validated at least one of the plurality of the users, wherein the generating the first certificate profile comprises recording and encoding a second certificate profile received from the at least one of the plurality of the users;

storing the generated first certificate profile in the information system;

applying a predetermined algorithm to generate a first identifier for an engineering artifact;

generating the at least one of the plurality of the engineering certificates from the second certificate profile and the engineering artifact;

retrieving from the information system the associated encrypted private key for the validated at least one of the plurality of the users; and

issuing a payload comprising the generated engineering certificate, the first identifier for the engineering artifact and the applied predetermined algorithm for the generating the first identifier for the engineering artifact, wherein the issuing the payload comprises:

receiving from a server the encrypted private key for the at least one of the plurality of the users;

decrypting the encrypted private key for the at least one of the plurality of the users, wherein the decrypting the encrypted private key generates a decrypted private key;

signing the payload for the engineering artifact using the decrypted private key;

validating the signed payload for the engineering artifact;

associating the signed payload for the engineering artifact with a public key for the at least one of the plurality of the users;

storing the signed payload for the engineering artifact and the associated public key in the information system; and

generating an operational status indicating the signed payload for the engineering artifact.

2. The method of claim 1, further comprising retrieving the at least one of the plurality of the issued engineering certificates.

3. The method of claim 2, wherein the retrieving the at least one of the plurality of the issued engineering certificates comprises:

receiving the first identifier for the engineering artifact for the at least one of the plurality of the users;

querying the information system for the signed engineering certificate using the first identifier for the engineering artifact and for the stored public key associated with the signed engineering certificate;

retrieving the signed engineering certificates and the stored public key associated with the signed engineering certificate; and

validating the retrieved signed engineering certificate using the stored public key associated with the signed engineering certificate.

4. The method of claim 1, wherein the third credential is a username and password.

5. The method of claim 1, wherein the third credential is a token.

6. The method of claim 1, wherein the identity provider generates a second identifier for the validated at least one of the plurality of the users.

7. The method of claim 6, wherein the storing in the information system the associated the encrypted private key for the validated at least one of the plurality of the users comprises:

generating a third identifier for the validated at least one of the plurality of the users;

associating the third identifier for the validated at least one of the plurality of the users with the second identifier generated by the identity provider for the validated at least one of the plurality of the users; and

storing in the information system the third identifier for the validated at least one of the plurality of the users with the second identifier generated by the identity provider for the validated at least one of the plurality of the users.

8. A system for managing engineering certificates, comprising:

one or more processors; and

one or more non-transitory computer-readable storage mediums in communication with the one or more processing systems and encoded with instructions for commanding the one or more processing systems to execute steps comprising:

determining whether an identity provider is a gateway to a plurality of first credentials;

providing a plurality of second credentials for a plurality of users, wherein the identity provider is not the gateway to the plurality of the first credentials;

authorizing access to an account for at least one of the plurality of the users using the plurality of the second credentials, wherein the authorizing the access to the account for the at least one of the plurality of the users comprises:

providing from the identity provider to the at least one of the plurality of the users an authentication challenge;

receiving by the identity provider from the at least one of the plurality of the users a third credential in response to the authentication challenge; and

validating by the identity provider the third credential received from the at least one of the plurality of the users;

activating the account for the validated at least one of the plurality of the users, wherein the activating the account for the validated at least one of the plurality of the users comprises:

generating an encrypted private key for the validated at least one of the plurality of the users;

associating the encrypted private key to the validated at least one of the plurality of the users; and

storing in an information system the associated encrypted private key for the validated at least one of the plurality of the users;

generating a first certificate profile for the validated at least one of the plurality of the users, wherein the generating the first certificate profile comprises recording and encoding a second certificate profile received from the at least one of the plurality of the users;

storing the generated first certificate profile in the information system;

applying a predetermined algorithm to generate a first identifier for an engineering artifact;

generating the at least one of the plurality of the engineering certificates from the second certificate profile and the engineering artifact;

retrieving from the information system the associated encrypted private key for the validated at least one of the plurality of the users; and

issuing a payload comprising the generated engineering certificate, the first identifier for the engineering artifact and the applied predetermined algorithm for the generating the first identifier for the engineering artifact, wherein the issuing the payload comprises:

receiving from a server the encrypted private key for the at least one of the plurality of the users;

decrypting the encrypted private key for the at least one of the plurality of the users, wherein the decrypting the encrypted private key generates a decrypted private key;

signing the payload for the engineering artifact using the decrypted private key;

validating the signed payload for the engineering artifact;

associating the signed payload for the engineering artifact with a public key for the at least one of the plurality of the users;

storing the signed payload for the engineering artifact and the associated public key in the information system; and

generating an operational status indicating the signed payload for the engineering artifact.

9. The system of claim 8, wherein the instructions for commanding the one or more processing systems to execute steps further comprises retrieving the at least one of the plurality of the issued engineering certificates.

10. The system of claim 9, wherein the retrieving the at least one of the plurality of the issued engineering certificates comprises:

receiving the first identifier for the engineering artifact for the at least one of the plurality of the users;

querying the information system for the signed engineering certificate using the first identifier for the engineering artifact and for the stored public key associated with the signed engineering certificate;

retrieving the signed engineering certificates and the stored public key associated with the signed engineering certificate; and

validating the retrieved signed engineering certificate using the stored public key associated with the signed engineering certificate.

11. The system of claim 8, wherein the third credential is a username and password.

12. The method of claim 8, wherein the third credential is a token.

13. The method of claim 8, wherein the identity provider generates a second identifier for the validated at least one of the plurality of the users.

14. The method of claim 13, wherein the storing in the information system the associated the encrypted private key for the validated at least one of the plurality of the users comprises:

generating a third identifier for the validated at least one of the plurality of the users;

associating the third identifier for the validated at least one of the plurality of the users with the second identifier generated by the identity provider for the validated at least one of the plurality of the users; and

storing in the information system the third identifier for the validated at least one of the plurality of the users with the second identifier generated by the identity provider for the validated at least one of the plurality of the users.

15. A non-transitory computer-readable medium storing a program causing a computer to execute a method for managing engineering certificates, the method comprising:

determining whether an identity provider is a gateway to a plurality of first credentials;

providing a plurality of second credentials for a plurality of users, wherein the identity provider is not the gateway to the plurality of the first credentials;

authorizing access to an account for at least one of the plurality of the users using the plurality of the second credentials, wherein the authorizing the access to the account for the at least one of the plurality of the users comprises:

providing from the identity provider to the at least one of the plurality of the users an authentication challenge;

receiving by the identity provider from the at least one of the plurality of the users a third credential in response to the authentication challenge; and

validating by the identity provider the third credential received from the at least one of the plurality of the users;

activating the account for the validated at least one of the plurality of the users, wherein the activating the account for the validated at least one of the plurality of the users comprises:

generating an encrypted private key for the validated at least one of the plurality of the users;

associating the encrypted private key to the validated at least one of the plurality of the users; and

storing in an information system the associated encrypted private key for the validated at least one of the plurality of the users;

generating a first certificate profile for the validated at least one of the plurality of the users, wherein the generating the first certificate profile comprises recording and encoding a second certificate profile received from the at least one of the plurality of the users;

storing the generated first certificate profile in the information system;

applying a predetermined algorithm to generate a first identifier for an engineering artifact;

generating the at least one of the plurality of the engineering certificates from the second certificate profile and the engineering artifact;

retrieving from the information system the associated encrypted private key for the validated at least one of the plurality of the users; and

issuing a payload comprising the generated engineering certificate, the first identifier for the engineering artifact and the applied predetermined algorithm for the generating the first identifier for the engineering artifact, wherein the issuing the payload comprises:

receiving from a server the encrypted private key for the at least one of the plurality of the users;

decrypting the encrypted private key for the at least one of the plurality of the users, wherein the decrypting the encrypted private key generates a decrypted private key;

signing the payload for the engineering artifact using the decrypted private key;

validating the signed payload for the engineering artifact;

associating the signed payload for the engineering artifact with a public key for the at least one of the plurality of the users;

storing the signed payload for the engineering artifact and the associated public key in the information system; and

generating an operational status indicating the signed payload for the engineering artifact.

16. The method of claim 15, further comprising retrieving the at least one of the plurality of the issued engineering certificates.

17. The method of claim 16, wherein the retrieving the at least one of the plurality of the issued engineering certificates comprises:

receiving the first identifier for the engineering artifact for the at least one of the plurality of the users;

querying the information system for the signed engineering certificate using the first identifier for the engineering artifact and for the stored public key associated with the signed engineering certificate;

retrieving the signed engineering certificates and the stored public key associated with the signed engineering certificate; and

validating the retrieved signed engineering certificate using the stored public key associated with the signed engineering certificate.

18. The method of claim 15, wherein the third credential is a username and password.

19. The method of claim 15, wherein the identity provider generates a second identifier for the validated at least one of the plurality of the users.

20. The method of claim 19, wherein the storing in the information system the associated the encrypted private key for the validated at least one of the plurality of the users comprises:

generating a third identifier for the validated at least one of the plurality of the users;

associating the third identifier for the validated at least one of the plurality of the users with the second identifier generated by the identity provider for the validated at least one of the plurality of the users; and

storing in the information system the third identifier for the validated at least one of the plurality of the users with the second identifier generated by the identity provider for the validated at least one of the plurality of the users.

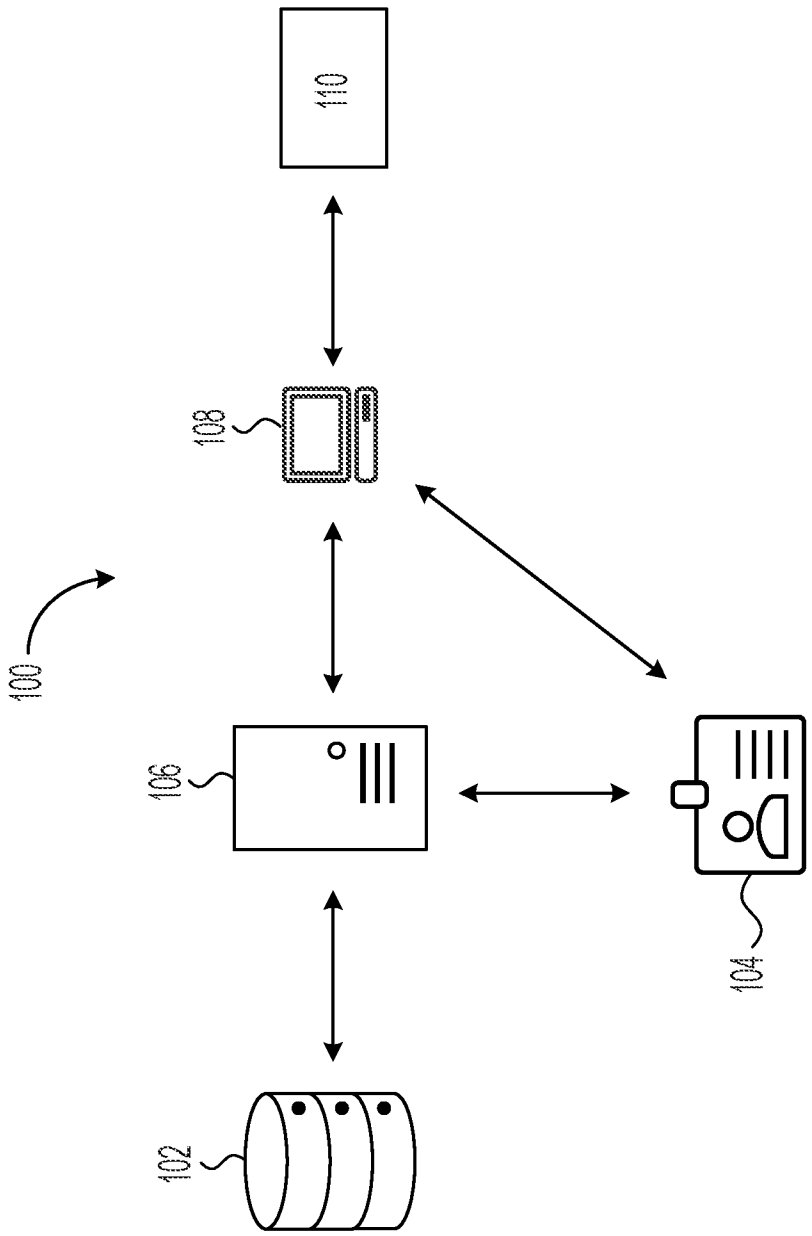

FIG. 1

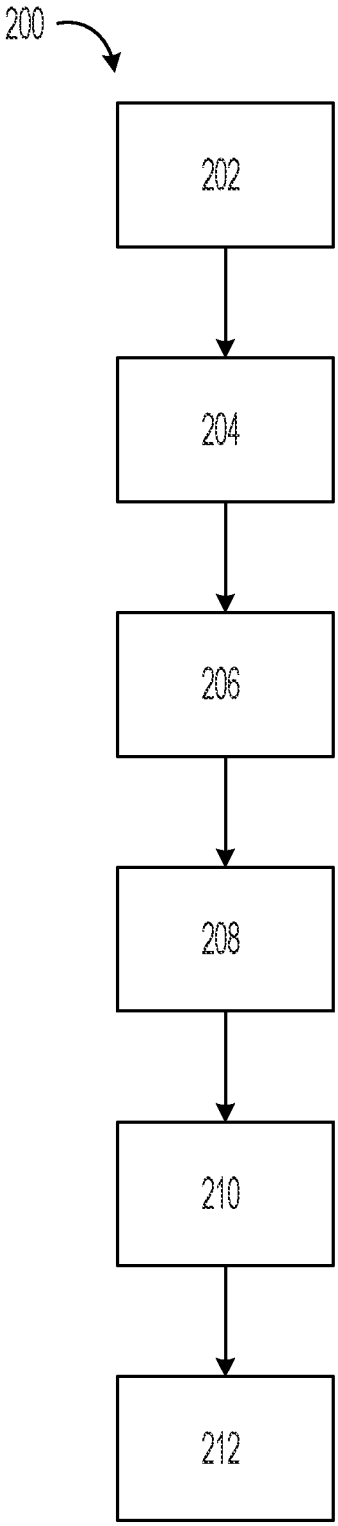

FIG. 2

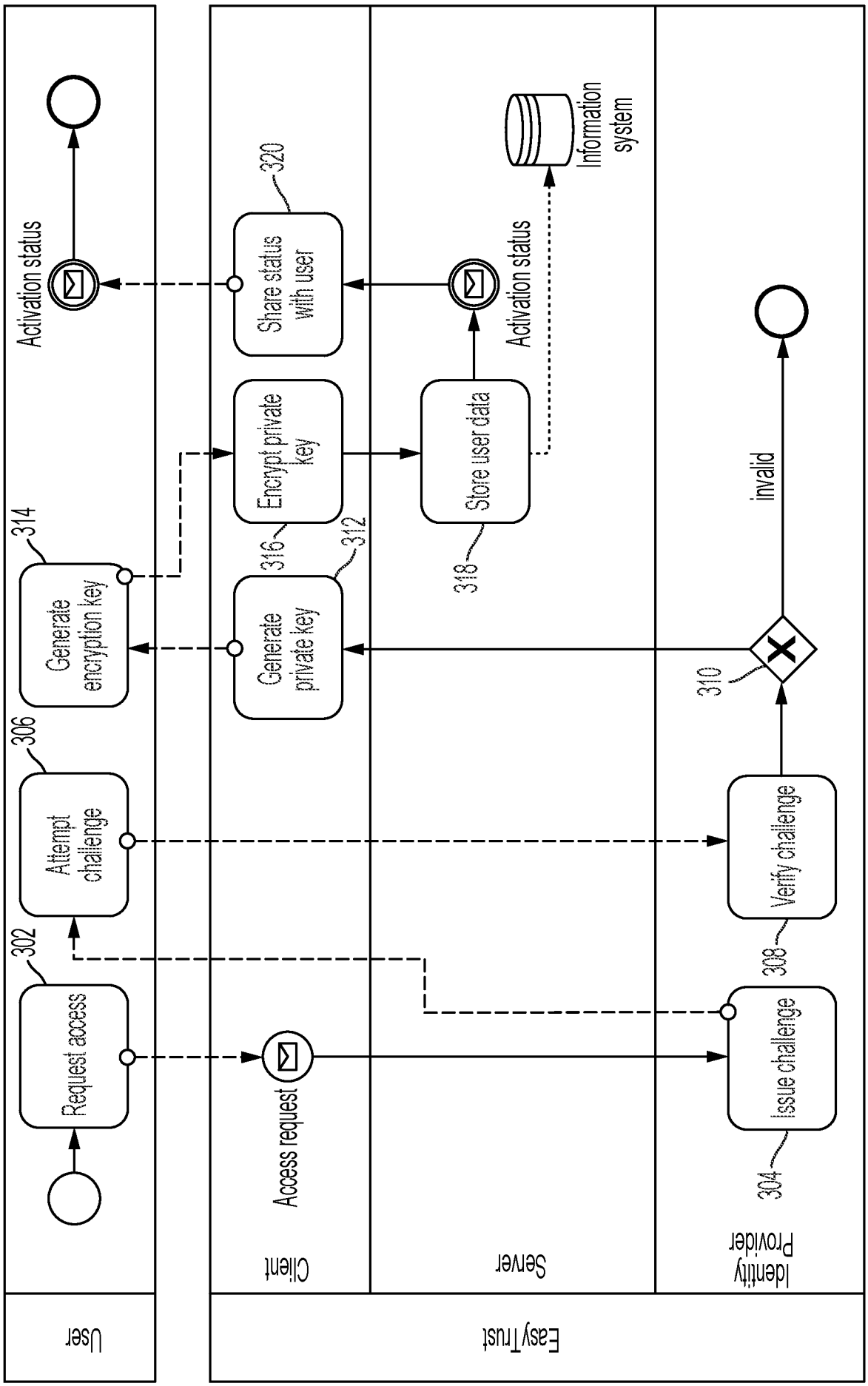
User
EasyTrust
Client
Server
Identity Provider
Request access
302
Attempt challenge
306
Generate encryption key
314
Activation status
Access request
Generate private key
312
Encrypt private key
316
Share status with user
320
Store user data
318
Activation status
Information system
Issue challenge
304
Verify challenge
308
invalid
310

FIG. 3

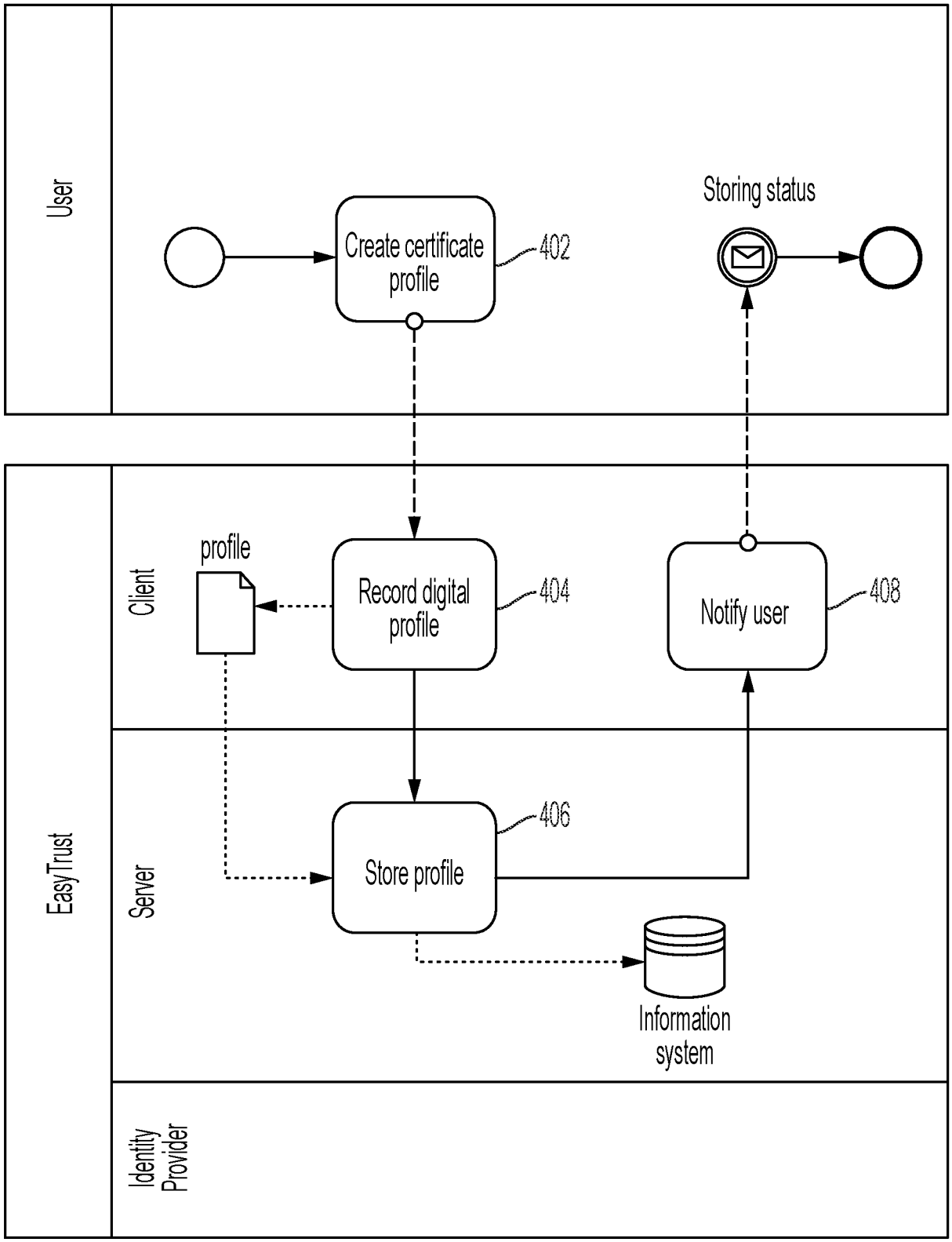
User
Create certificate profile
402
Storing status
EasyTrust
Client
profile
Record digital profile
404
Notify user
408
Server
406
Store profile
Information system
Identity Provider

FIG. 4

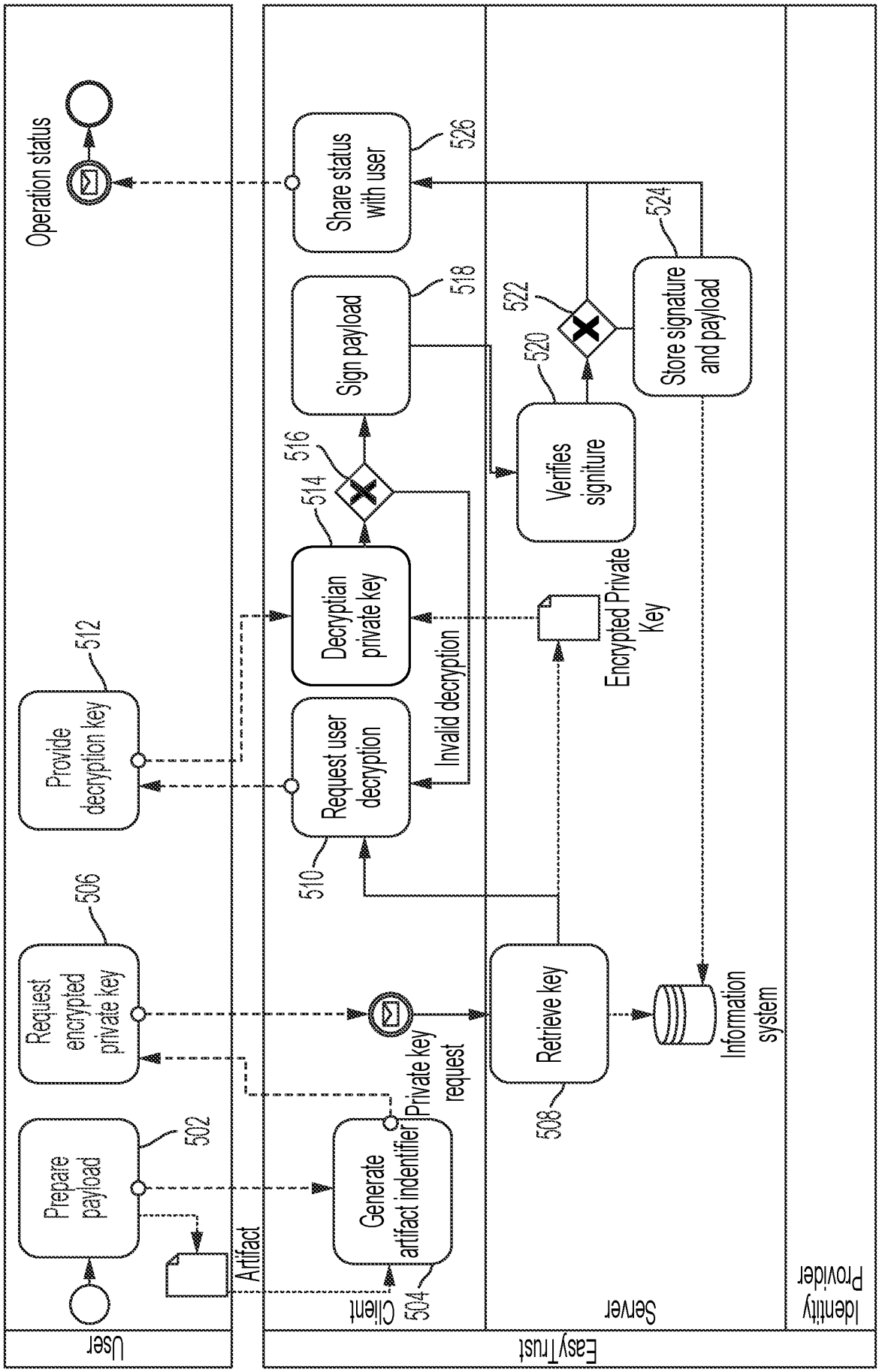
EasyTrust
User
Client
Server
Identity Provider
Prepare payload
502
Artifact
Generate artifact indentifier
504
Request encrypted private key
506
Private key request
Provide decryption key
512
Request user decryption
510
Invalid decryption
Decryptian private key
514
516
Sign payload
518
Share status with user
526
Operation status
Retrieve key
508
Information system
Encrypted Private Key
Verifies signiture
520
522
Store signature and payload
524

FIG. 5

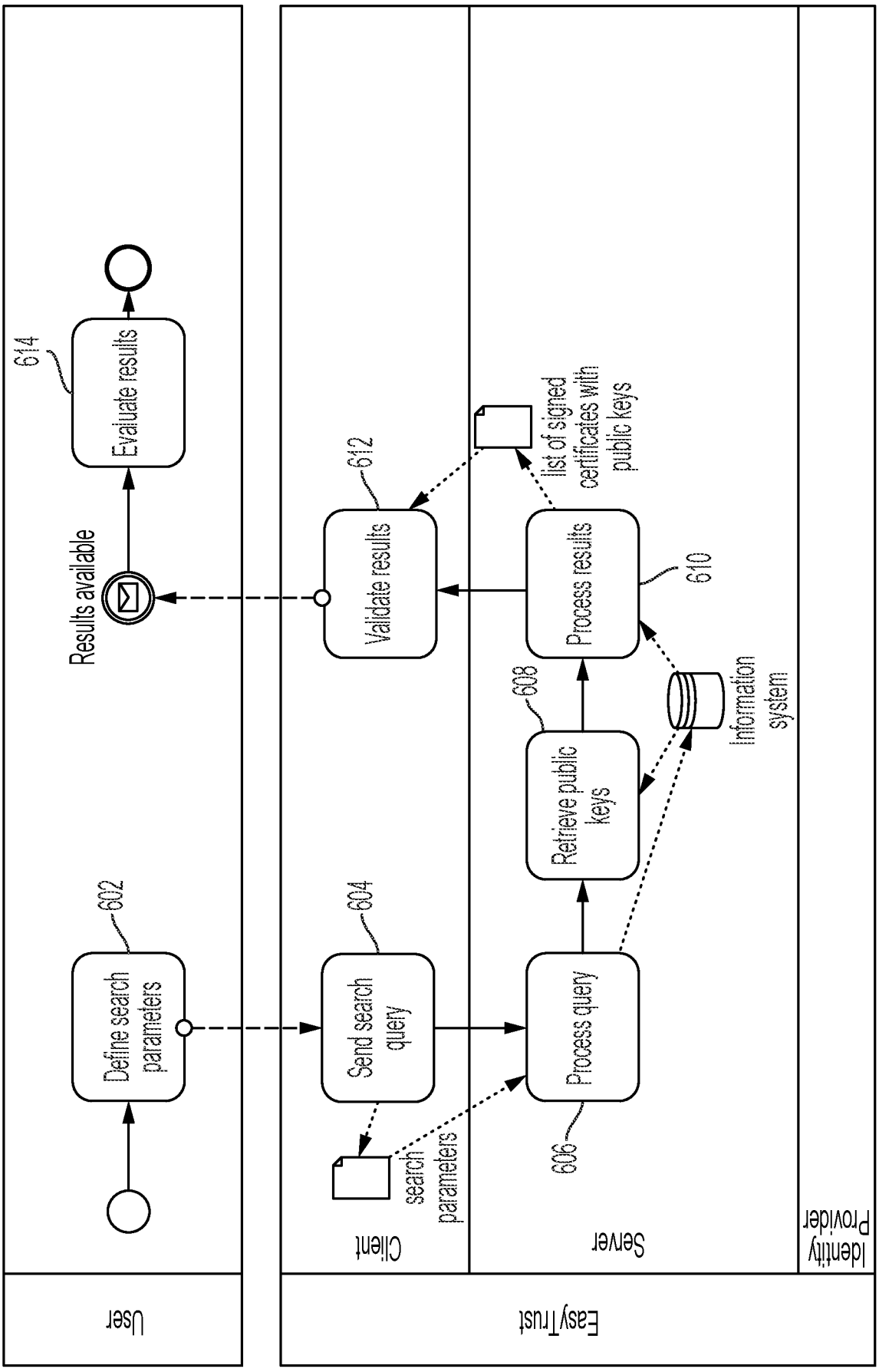
User
EasyTrust
Client
Server
Identity Provider
Define search parameters
602
Send search query
604
search parameters
Process query
606
Retrieve public keys
608
Information system
Process results
610
list of signed certificates with public keys
Validate results
612
Results available
Evaluate results
614

FIG. 6