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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 October 2013 (03.10.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/147732 A1

(51) International Patent Classification:
H04L 9/08 (2006.01) *G06F 21/62* (2013.01)
H04L 9/32 (2006.01)

(21) International Application Number:
PCT/US2012/030516

(22) International Filing Date:
26 March 2012 (26.03.2012)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **SIEMENS AKTIENGESELLSCHAFT** [DE/DE]; Wittelsbacherplatz 2, 80333 Munich (DE).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **CRAWFORD, John W.** [US/US]; 3084 Antioch Road, Johnson City, Tennessee 37604 (US). **KYLES, Ronald** [US/US]; 99 Walton Street, Jonesborough, Tennessee 37659 (US).

(74) Agents: **EVENSEN, Andrea L.** et al.; Siemens Corporation- Intellectual Property Dept., 170 Wood Avenue South, Iselin, New Jersey 08830 (US).

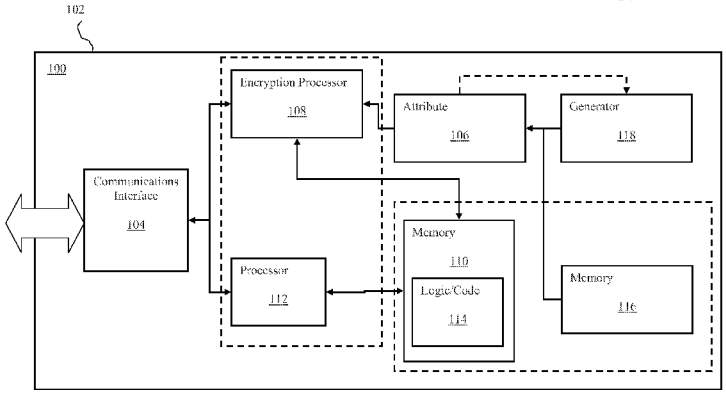
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report (Art. 21(3))*

(54) **Title**: PROGRAMMABLE LOGIC CONTROLLER HAVING EMBEDDED DYNAMIC GENERATION OF ENCRYPTION KEYS

FIG. 1



(57) **Abstract**: The disclosed embodiments relate to a programmable logic controller ("PLC") having embedded encryption key generation capability for generating symmetrical keys or asymmetrical key pairs unique to the PLC. The PLC unique encryption keys may then be used to secure communication with the particular PLC and/or to validate executable program code prior to execution thereof by the intended PLC.

WO 2013/147732 A1

PROGRAMMABLE LOGIC CONTROLLER HAVING EMBEDDED DYNAMIC GENERATION OF ENCRYPTION KEYS

BACKGROUND

[0001] A programmable logic controller ("PLC") or programmable controller is a digital computer used for automation of electromechanical processes, such as control of machinery on factory assembly lines, amusement rides, or light fixtures. PLCs are used in many industries and machines. Unlike general-purpose computers, the PLC is designed for multiple inputs and output arrangements, extended temperature ranges, immunity to electrical noise, and resistance to vibration and impact. Programs to control machine operation are typically stored in battery-backed-up or non-volatile memory. A PLC is an example of a hard real time system since output results must be produced in response to input conditions within a limited time, otherwise unintended operation will result.

[0002] The main difference from other computers is that PLCs are typically armored for severe conditions (such as dust, moisture, heat, cold) and have the facility for extensive input/output (I/O) arrangements to connect, for example, to sensors and actuators. PLCs may be capable of reading limit switches, analog process variables (such as temperature and pressure), and the positions of complex positioning systems. Some PLCs may use machine vision and/or may operate electric motors, pneumatic or hydraulic cylinders, magnetic relays, solenoids, or analog outputs. The input/output arrangements may be built into a simple PLC, or the PLC may have external I/O modules, which may be referred to as "signal modules," attached to a computer network that plugs into the PLC.

[0003] Modular PLCs may include a chassis (also called a rack) into which are placed modules with different functions. The processor and selection of I/O modules are customized for the particular application. Several racks may be administered by a single processor, and may have thousands of inputs and outputs. A communications medium, such as a special high speed serial I/O link, may be used so that racks can be distributed away from the processor, reducing the wiring costs for large plants.

[0004] PLCs may be used in mission critical environments where failures may compromise worker, public and/or environmental safety or otherwise result in substantial costs. As such, some PLC's may be designed with fail-safe and/or security features. Regardless, proper installation and configuration of such PLC's may be required to ensure correct operation as well as, for example, compliance with regulatory requirements.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] Figure 1 depicts a block diagram of an exemplary programmable logic controller according to the disclosed embodiments.

[0006] Figure 2 shows a flow chart depicting operation of the programmable logic controller of Figure 1 according to one embodiment.

[0007] Figure 3 shows a flow chart depicting operation of the programmable logic controller of Figure 1 according to another embodiment.

[0008] Figure 4 shows a block diagram of a general computer system for use with the disclosed embodiments.

DETAILED DESCRIPTION

[0009] The disclosed embodiments relate to a programmable logic controller ("PLC") having embedded encryption key generation capability for generating symmetrical keys and/or asymmetrical key pairs unique to the PLC. The PLC unique encryption keys may then be used to secure communication with the particular PLC and/or to validate executable program code prior to installation and/or execution thereof by the intended PLC.

[0010] Generally, it may be desirable to communicate with a PLC in a secure and reliable manner to monitor, control or otherwise modify the PLC or the operation thereof. For PLCs deployed in mission critical, hazardous or other environments where secure, safe and/or reliable operation is desirable, secure communications, such as encrypted communications, ensure that only authorized access to the PLC is provided. For multiple PLCs deployed in a particular

environment, it is desirable to ensure that communications with a particular PLC are, in fact, occurring with intended PLC and not with a different PLC.

[0011] Further, as was described above, PLCs generally execute control programs to perform their functions. For PLCs deployed in mission critical, hazardous or other environments where secure, safe and/or reliable operation is desirable, ensuring that the control programs are authorized, uncorrupted or otherwise valid may be desirable. Validation mechanisms, such as code or header encryption or signing, may be provided which allow the PLC to validate a control program prior to installation and/or execution. Ensuring that the control program is being executed on the intended PLC may be further desirable to ensure intended operation. For control programs developed by the third party developers and provided to the PLC operator, such as for a license fee, these same validation mechanisms may be utilized to prevent unauthorized modifications to the control program and/or unauthorized, e.g. unlicensed use, such as on unauthorized PLCs. In addition, verification/authentication and secure communications/encipherment capabilities may be provided.

[0012] As discussed above, typically encryption mechanisms are utilized to secure communications and/or implement executable code validation. Such encryption mechanisms may include both symmetrical and asymmetrical key based mechanisms. Once example of an asymmetrical key based encryption mechanism is public key cryptography which utilizes an asymmetrical key pair including a public encryption key and a private encryption key. Messages encrypted with the public encryption key, which is shared, may only be decrypted with the private encryption key, which is not shared. Asymmetrical key based encryption mechanisms may facilitate secure unidirectional communication as well as authentication functions and further, where entities exchange public encryption keys, bidirectional communication, each direction using the key pair of the receiver, may be implemented. Symmetrical key based encryption mechanisms utilize a single encryption key which is shared and which may be

used to both encrypt and decrypt messages. Symmetrical key based encryption mechanisms may be useful for securing bidirectional communications.

[0013] One way of implementing the above described encryption mechanisms with respect to PLCs is to generate the encryption key(s) using a third party device, service or software and the provide the key(s) to the PLC, e.g. by programming or otherwise communicating it to the PLC, and to the entity or device which will be communicating with that PLC. The provisioning of the encryption key(s) then facilitates the desired secure operation.

[0014] However, generating encryption keys in this manner and then providing them to the PLC leaves them vulnerable to errors, interception or manipulation which may compromise the desired secure operation. For example, PLC control programs are typically developed using a software development program executing a tradition workstation computer. When the programmer completes development of the control program, they may then use the software development program to generate the necessary encryption key(s) to secure the control program code. However, it is known that these software development tools can be reverse engineered to derive the encryption key algorithms or the encryption keys themselves allowing any security to be circumvented. Further, if the PLC loses power, resets or is otherwise restarted, any encryption keys stored therein may be lost and will need to be replaced.

[0015] As introduced above, the disclosed embodiments relate to a PLC having embedded encryption key generation functionality which is uniquely tied to the particular PLC, as will be explained. As a PLC is typically more secure than workstation computer, access to the encryption algorithm or any encryption keys stored within the PLC is more secure. Further, as the encryption key generation functionality is uniquely tied to the particular PLC, communications and/or executable program code secured using an encryption key generated by the PLC may only be utilized with that particular PLC. Further, the likelihood that two PLCs will generate identical encryption keys is substantially reduced if not eliminated. In addition the unique association of the PLC with the encryption keys

enables the PLC to recreate the encryption keys following a loss of power, reset or other restart of the PLC.

[0016] Herein, the phrase "coupled with" is defined to mean directly connected to or indirectly connected through one or more intermediate components. Such intermediate components may include both hardware and software based components. Further, to clarify the use in the pending claims and to hereby provide notice to the public, the phrases "at least one of <A>, <B>, ... and <N>" or "at least one of <A>, <B>, ... <N>, or combinations thereof" are defined by the Applicant in the broadest sense, superseding any other implied definitions herebefore or hereinafter unless expressly asserted by the Applicant to the contrary, to mean one or more elements selected from the group comprising A, B, ... and N, that is to say, any combination of one or more of the elements A, B, ... or N including any one element alone or in combination with one or more of the other elements which may also include, in combination, additional elements not listed.

[0017] Figure 1 shows a block diagram of an exemplary PLC 100 according to the disclosed embodiments. The PLC 100 includes a housing 102, one or more communications interfaces 104, an encryption processor 108 coupled with the communications interfaces 104 and an attribute 106 coupled with the encryption processor 108. It will be appreciated that the PLC 100 may be implemented as computing device, such as the computing device 400 described below with respect to Figure 4 and wherein the communications interfaces 104 may be implemented as the described communications interface 418 and the encryption processor 108 may be implemented as the processor 402. The housing 102 may enclose at least the attribute 106 and the encryption processor 108 wherein the communications interfaces further facilitate communications through the housing 102 with devices external thereto. In one embodiment, the PLC 100 may be implemented in a modular implementation as a CPU module, such as the Siemens Simatic S7 modular CPU manufactured by Siemens AG, located in Munich, Germany, which then connects to one or more signal or other modules to implement the desired

control functions. In this implementation, the PLC 100 may be the CPU module alone which houses the processor 108 and other components and may utilize the disclosed embodiments for communication with the external modules. In alternate implementation, the PLC 100 may be a self contained system for implementing the desired control functions.

[0018] In particular, the communications interface 104 is operative to communicate data between the PLC 100 and a device external thereto and may include a wired or wireless network interface, such as a serial interface, Wi-Fi interface, cellular interface, etc. The communication interface 104 may further implement suitable communications protocols for communicating with external devices, such as Ethernet, Modbus, TCP/IP, etc. The communications interface 104 may be utilized to communicate operational data between the PLC 100 and external devices, such as management consoles, etc. The communications interface 104 may be further utilized to configure, control and a generally communicate with the PLC 100 as described herein.

[0019] The attribute 106 is characterized by a value unique to the PLC 100. In one embodiment, the value of the attribute 106 is imputed to the PLC 100 during manufacture or otherwise during provisioning thereof. For example, the attribute 106 may include a serial number or other unique identifier, the value of which is stored, during manufacture, deployment or provisioning, in a memory 116, which may be volatile or non-volatile and may be implemented as the memory 404 or drive unit 406 described below with respect to Figure 4. Alternatively, or in addition thereto, the attribute 106 may be a physical characteristic of the PLC 100 such as a resistance value, circuit delay value or other unique attribute which, for example, may result from manufacturing or environmental variances or tolerances. Further still, the attribute 106 may be a logically unique characteristic derived from other devices in communication with the PLC 100 and/or via one or more sensors coupled with the PLC 100. In one embodiment, the attribute 106 may further include a generator 118, coupled with the unique physical or logical characteristic 106, which generates the unique value as a function of the physical

or logical characteristic 106. For example the generator may measure or read the value of the physical characteristic and convert it to a digital value representative thereof. The generator 118 may include an analog measurement sampler, circuit or calculator which samples or measures the value of the physical characteristic, coupled with an analog to digital converter to convert the sampled or measured value to a digital representation thereof. It will be appreciated that physical attributes whose value may vary with changes in environmental conditions of the environment in which the PLC 100 is deployed may require compensation mechanisms, which may implemented as part of the generator 118, to ensure a consistent value thereof, as will be described. For example, where a resistance or delay attribute is utilized, thermal or wear compensation may need to be provided within the PLC 100 to ensure a consistent value is sampled or otherwise measured within the deployment environment. Alternatively, the generator 118 may compute or otherwise derive the unique attribute 106 such as by identifying a unique pattern of devices in communication with the PLC 100 or a unique set of environmental characteristics sensed by sensors coupled with the PLC 100. It is desirable that the value of attribute 106 not be discernable external to the PLC 100 or, at least, be difficult to discern. Generally, the value of the attribute 106 should be a secret to the PLC 100 and therefore is, at least, not communicated via communications interface 104 or visible external to the housing 102 of the PLC 100. It will be appreciated that the degree to which the value of the attribute 106 is kept secret or otherwise confidential is implementation dependent and may depend on the level of security desired. It is desirable that the attribute 106 value be a constant, or otherwise consistently reproducible, such that, as will be described, encryption keys may be regenerated, such as to replicate them after a power failure, reset, reboot, etc.

[0020] The encryption processor 108 is coupled between the attribute 106 and the communications interface 104 and is operative to generate an encryption key unique to the PLC 100 based at least on the unique value of the attribute 106 and communicate the encryption key via the communications interface 104 to, for

example, a requestor of an encryption key as will be described. It will be appreciated that the encryption processor 108 may be a general purpose processor, such as the processor 402 described below with respect to Figure 4 and may be the central processor of the PLC 100 which, in addition to the functions described herein, further generally performs the functions of the PLC 100 such by executing one or more control programs to control and/or monitor devices coupled with the PLC 100 via the communications interfaces 104. Accordingly, the functionality described herein may be implemented as computer executable program code and/or logic stored in the memory 110 and executable by the processor 108 to cause the processor 108 to perform the described functions. The encryption processor 108 may implement various symmetrical and/or asymmetrical encryption key generation algorithms, such as public key algorithms as are known. By factoring in the PLC-unique attribute 106 value, which may be combined with another seed value, such as a user provided password, time code or other value, encryption keys which are unique to the PLC 100 may be generated. In one embodiment, the encryption processor 108 is operative to generate either symmetrical or asymmetrical encryption keys. As will be described, the generated encryption key(s) may then be stored in a memory 110 for later use as will be described. It will be appreciated the memory 110 may be the memory 404 or drive unit 406 described below with respect to Figure 4 which may further be used for general operation of the PLC 100, such as for storing control programs, data and other parameters, etc. Alternatively, memory 110 may be a separate memory for exclusive storage of encryption keys and may be secure or otherwise hardened against unauthorized access or tampering.

[0021] As used herein, encryption not only refers to obfuscation of an entire message but also to "digital signing" or authentication, alone, e.g. the message is sent in plain text, or in combination with message obfuscation, whereby only a portion or an attribute of a message is encrypted, such as a hash value. Whereby, the encryption allows the PLC 100 to authenticate or otherwise validate the message content as being intended for the PLC 100, as being unmodified, as

originating from a trusted source, or a combination thereof. Accordingly, the use of the term decryption may refer to de-obfuscating a message, authenticating the content thereof, validating the integrity of the message content, evaluating the integrity of the message originator, or combinations thereof.

[0022] In one embodiment, the encryption processor 108 may be further operative to generate a symmetrical encryption key and communicate that symmetrical encryption key to one or more external devices which wish to communicate with the PLC 100. The encryption processor 108 may then be further operative to encrypt communications to be transmitted via the communication interface 104 using the encryption key, decrypt communications received thereby using the encryption key, or combinations thereof. It will be appreciated that the encryption or decryption of communications may be performed by a component other than the encryption processor 108, such as the communications interfaces 104 which may perform the encryption/decryption as communications pass there through. It will be appreciated the encryption processor 108 may generate multiple different symmetrical keys, each for use for communicating with a different external device. In this way, the PLC 100 can segregate communications. Further, if one encryption key is compromised or communications with the particular external device are no longer necessary, the particular encryption key can be disabled or otherwise decommissioned. It will be appreciated that in a multiple-encryption key implementation, the PLC 100, upon receipt of a communication, may attempt to apply each available encryption key to the communication until it is successfully decrypted or all available keys have been exhausted. Alternatively, the PLC 100 may generate or otherwise assign external device identifiers identifying each external device and associating a particular encryption key with the device such that communications with that device are further identified using the associated identifier. Accordingly, the PLC 100 upon receipt of a communication may determine the identifier and utilize the identifier to determine which encryption key to use. In one embodiment, this identifier may include the network address, such as the IP address or Modbus

address, of the external device. Where a device is only sending communication to the PLC 100, an asymmetrical key pair may be generated whereby the device encrypts the communication using the public encryption key and the PLC 100 decrypts the communications using the private encryption key. It will be appreciated that asymmetrical encryption keys may be used for bidirectional communication where the PLC 100 is further provided with the public encryption key associated with the particular external device to which the communications are to be sent.

[0023] In one embodiment the encryption processor 108 is further operative to generate an encryption key pair including public encryption key and an associated private encryption key, based at least on the attribute, the private encryption key being stored in the memory 110 coupled with the encryption processor 108 internal to the PLC 100. The public encryption key may then be communicated via the communications interfaces 104 to a requestor. For example, in one embodiment, the PLC 100, or its primary processor 112, which may be the same as the encryption processor 108 and which is coupled with the communications interface 104, may be operative to receive executable program code to be executed thereby via the communications interface 104, store the received executable program code in a memory 110 coupled therewith and validate the stored received executable program code using the encryption key before execution thereof by the processor 112. In particular, a software developer may request a public encryption key from the PLC 100 to encrypt or otherwise digitally sign their executable program code, or a portion thereof such as a code block header, etc., and then send that code to the PLC 100 for execution. Upon receipt, the PLC 100 validates, e.g. decrypts or otherwise authenticates, the code prior to execution using the associated private encryption key. In one embodiment, the PLC 100 validates the code before storing it in the memory 110 for subsequent execution. Further, once validated, the code may be stored in an unencrypted form, requiring no further decryption or authentication to execute, or in an encrypted form wherein each execution requires revalidation. Alternatively, the encrypted code may be stored

and revalidated each time it is executed. In this manner, a developer and/or operator of the PLC 100 can ensure that the program code is not tampered with or otherwise corrupted or modified and/or that it is utilized only on the intended PLC 100 and is not, for example, deployed to other unintended PLCs as other PLCs would not possess the proper private encryption key so as to be able to decrypt the program code.

[0024] It will be appreciated that limited modes of program execution, such as evaluation, test or debug modes, or other secure execution modes, may be implemented whereby unvalidated computer program code may be executed on the PLC 100.

[0025] In one embodiment, the encryption processor 108 is further operative to generate the encryption key(s) in response to a request received thereby via the communications interface 104. For example, a device wishing to communicate with the PLC 100 may initiate a request for an encryption key. In another example, a software developer wishing to generate executable code for execution by the PLC 100 may initiate a request for an encryption key.

[0026] It will be appreciated that additional protocols may be implemented for securely communicating the encryption keys. For example, a key-exchange protocol may be established between the PLC 100 and the external device to exchange keys, such as symmetrical keys, using messages encrypted using asymmetrical keys. This may ensure that the communication of the encryption key is not compromised.

[0027] Figure 2 depicts a flow chart showing operation of the PLC 100 of Figure 1 for facilitating secure integrity of a PLC 100. In particular, the operation includes: receiving, by a processor 108, a value of an attribute 106 unique to the PLC 100 which is not communicated via a communications interface 104 of the PLC 100 operative to communicate data between the PLC 100 and a device external thereto [block 202]; generating, by the processor 108, an encryption key unique to the PLC 100 based at least in part on the unique value [block 204]; and

communicating, by the processor 100, the encryption key via the communications interface 104 [block 206].

[0028] In one embodiment, the operation further includes enclosing the processor 108 within a housing 102 in which at least the attribute 106 is located, the communications interface 104 being further operative to communicate data through the housing 102 [block 208].

[0029] In one embodiment, the operation further includes storing the unique value of the attribute 106 in a memory 116 coupled with the processor 108 [block 210].

[0030] In one embodiment wherein the PLC 100 is characterized by a physical characteristic unique thereto, the operation further includes generating the unique value as a function of the unique physical characteristic [block 212]. The operation may further include compensating for an environmental condition which may affect the value of the unique physical characteristic.

[0031] In one embodiment, wherein the encryption key comprises a public encryption key of a key pair , the operation may further include generating a private encryption key of the key pair associated with the public encryption key based at least on the unique value [block 214], and storing the private key in a memory 110 coupled with the processor 108 [block 216].

[0032] In one embodiment, the operation may further include storing, by the processor, the encryption key in a memory 110 internal to the PLC 100 and coupled with the processor 108 [block 218].

[0033] In one embodiment, the operation may further include: encrypting, by the processor 108 communications to be transmitted by the communications interface 104 using the encryption key [block 220]; or decrypting, by the processor 108, communications received by the communications interface 104 using the encryption key [block 222].

[0034] In one embodiment, the operation may further include: receiving, by the processor 108 via the communications interface 104, executable computer program code for execution by the PLC 100 [block 224]; storing, by the processor

108, the received executable computer program code in a memory 110 coupled therewith [block 226]; validating, by the processor 108, the received executable computer program code based on the encryption key [block 228]; and executing the stored received executable computer program code only if validated [block 230] .

[0035] In one embodiment, the operation may further include: receiving, by the processor 108 via the communications interface 104, a request to generate the encryption key [block 232]; and wherein the generating further comprises generating the encryption key responsive to the request [block 204].

[0036] Figure 3 depicts a flow chart showing exemplary operation of the PLC 100 of Figure 1 according to one embodiment. In particular, upon receipt of a request to generate an encryption key or key pair, which may or may not also include a password to be incorporated therein [block 302], the PLC 100 determines whether the request for a symmetric encryption key or an asymmetric encryption key pair [block 306]. The password, if provided, may be cryptographically hashed to create an initialization vector and provided to the encryption processor [blocks 304 and 308]. Further PLC 100 unique attribute 108 value is obtained by the encryption processor [block 314]. Depending upon the request, a symmetric encryption key or asymmetric encryption key pair is generated, factoring the unique attribute 108 value and the hashed password, if provided [blocks 310 and 312]. Once generated, the symmetric encryption key or public encryption key is then returned to the requestor [block 316]. If the request was for an asymmetric key pair, the private encryption key is stored in a memory 110.

[0037] In one exemplary implementation whereby a PLC control program developer has developed code that they wish to protect and has caused their development software to request an encryption key from the PLC 100 with, for example, a password, and subsequently received an encryption key responsive to their request as detailed above, the development software then encrypt the program code using the supplied encryption key. For example, the development

software may then create a code block header which contains the password hash and an integrity checksum of the combined password hash and code block. The header and the protected code may then be communicated to the PLC 100 which then decrypts the protected code prior to execution thereof.

[0038] One skilled in the art will appreciate that one or more components described herein may be implemented using, among other things, a tangible computer-readable medium comprising computer-executable instructions (e.g., executable software code). Alternatively, modules may be implemented as software code, firmware code, hardware, and/or a combination of the aforementioned. For example the modules may be embodied as part of a programmable logic controller as described above.

[0039] Referring to Figure 40, an illustrative embodiment of a general computer system 400 is shown. The computer system 400 can include a set of instructions that can be executed to cause the computer system 400 to perform any one or more of the methods or computer based functions disclosed herein. The computer system 400 may operate as a standalone device or may be connected, e.g., using a network, to other computer systems or peripheral devices. Any of the components discussed above, such as the PLC 100 or a component thereof, may be a computer system 400 or a component in the computer system 400. The computer system 400 may implement a programmable logic controller, of which the disclosed embodiments are a component thereof.

[0040] In a networked deployment, the computer system 400 may operate in the capacity of a server or as a client user computer in a client-server user network environment, or as a peer computer system in a peer-to-peer (or distributed) network environment. The computer system 400 can also be implemented as or incorporated into various devices, such as a personal computer (PC), a tablet PC, a set-top box (STB), a personal digital assistant (PDA), a mobile device, a palmtop computer, a laptop computer, a desktop computer, a communications device, a wireless telephone, a land-line telephone, a control system, a camera, a scanner, a facsimile machine, a printer, a pager, a personal trusted device, a web appliance, a

network router, switch or bridge, or any other machine capable of executing a set of instructions (sequential or otherwise) that specify actions to be taken by that machine. In a particular embodiment, the computer system 400 can be implemented using electronic devices that provide voice, video or data communication. Further, while a single computer system 400 is illustrated, the term "system" shall also be taken to include any collection of systems or sub-systems that individually or jointly execute a set, or multiple sets, of instructions to perform one or more computer functions.

[0041] As illustrated in Figure 4, the computer system 400 may include a processor 402, e.g., a central processing unit (CPU), a graphics processing unit (GPU), or both. The processor 402 may be a component in a variety of systems. For example, the processor 402 may be part of a standard personal computer or a workstation. The processor 402 may be one or more general processors, digital signal processors, application specific integrated circuits, field programmable gate arrays, servers, networks, digital circuits, analog circuits, combinations thereof, or other now known or later developed devices for analyzing and processing data. The processor 402 may implement a software program, such as code generated manually (i.e., programmed).

[0042] The computer system 400 may include a memory 404 that can communicate via a bus 408. The memory 404 may be a main memory, a static memory, or a dynamic memory. The memory 404 may include, but is not limited to computer readable storage media such as various types of volatile and non-volatile storage media, including but not limited to random access memory, read-only memory, programmable read-only memory, electrically programmable read-only memory, electrically erasable read-only memory, flash memory, magnetic tape or disk, optical media and the like. In one embodiment, the memory 404 includes a cache or random access memory for the processor 402. In alternative embodiments, the memory 404 is separate from the processor 402, such as a cache memory of a processor, the system memory, or other memory. The memory 404 may be an external storage device or database for storing data. Examples include

a hard drive, compact disc ("CD"), digital video disc ("DVD"), memory card, memory stick, floppy disc, universal serial bus ("USB") memory device, or any other device operative to store data. The memory 404 is operable to store instructions executable by the processor 402. The functions, acts or tasks illustrated in the figures or described herein may be performed by the programmed processor 402 executing the instructions 412 stored in the memory 404. The functions, acts or tasks are independent of the particular type of instructions set, storage media, processor or processing strategy and may be performed by software, hardware, integrated circuits, firm-ware, micro-code and the like, operating alone or in combination. Likewise, processing strategies may include multiprocessing, multitasking, parallel processing and the like.

[0043] As shown, the computer system 400 may further include a display unit 414, such as a liquid crystal display (LCD), an organic light emitting diode (OLED), a flat panel display, a solid state display, a cathode ray tube (CRT), a projector, a printer or other now known or later developed display device for outputting determined information. The display 414 may act as an interface for the user to see the functioning of the processor 402, or specifically as an interface with the software stored in the memory 404 or in the drive unit 406.

[0044] Additionally, the computer system 400 may include an input device 416 configured to allow a user to interact with any of the components of system 400. The input device 416 may be a number pad, a keyboard, or a cursor control device, such as a mouse, or a joystick, touch screen display, remote control or any other device operative to interact with the system 400.

[0045] In a particular embodiment, as depicted in Figure 4, the computer system 400 may also include a disk or optical drive unit 406. The disk drive unit 406 may include a computer-readable medium 410 in which one or more sets of instructions 412, e.g. software, can be embedded. Further, the instructions 412 may embody one or more of the methods or logic as described herein. In a particular embodiment, the instructions 412 may reside completely, or at least partially, within the memory 404 and/or within the processor 402 during execution

by the computer system 400. The memory 404 and the processor 402 also may include computer-readable media as discussed above.

[0046] The present disclosure contemplates a computer-readable medium that includes instructions 412 or receives and executes instructions 412 responsive to a propagated signal, so that a device connected to a network 420 can communicate voice, video, audio, images or any other data over the network 420. Further, the instructions 412 may be transmitted or received over the network 420 via a communication interface 418. The communication interface 418 may be a part of the processor 402 or may be a separate component. The communication interface 418 may be created in software or may be a physical connection in hardware. The communication interface 418 is configured to connect with a network 420, external media, the display 414, or any other components in system 400, or combinations thereof. The connection with the network 420 may be a physical connection, such as a wired Ethernet connection or may be established wirelessly as discussed below. Likewise, the additional connections with other components of the system 400 may be physical connections or may be established wirelessly.

[0047] The network 420 may include wired networks, wireless networks, or combinations thereof. The wireless network may be a Modbus network, cellular telephone network, an 802.11, 802.16, 802.20, or WiMax network. Further, the network 420 may be a public network, such as the Internet, a private network, such as an intranet, or combinations thereof, and may utilize a variety of networking protocols now available or later developed including, but not limited to TCP/IP based networking protocols.

[0048] Embodiments of the subject matter and the functional operations described in this specification can be implemented in digital electronic circuitry, or in computer software, firmware, or hardware, including the structures disclosed in this specification and their structural equivalents, or in combinations of one or more of them. Embodiments of the subject matter described in this specification can be implemented as one or more computer program products, i.e., one or more modules of computer program instructions encoded on a computer readable

medium for execution by, or to control the operation of, data processing apparatus. While the computer-readable medium is shown to be a single medium, the term "computer-readable medium" includes a single medium or multiple media, such as a centralized or distributed database, and/or associated caches and servers that store one or more sets of instructions. The term "computer-readable medium" shall also include any medium that is capable of storing, encoding or carrying a set of instructions for execution by a processor or that cause a computer system to perform any one or more of the methods or operations disclosed herein. The computer readable medium can be a machine-readable storage device, a machine-readable storage substrate, a memory device, or a combination of one or more of them. The term “data processing apparatus” encompasses all apparatus, devices, and machines for processing data, including by way of example a programmable processor, a computer, or multiple processors or computers. The apparatus can include, in addition to hardware, code that creates an execution environment for the computer program in question, e.g., code that constitutes processor firmware, a protocol stack, a database management system, an operating system, or a combination of one or more of them.

[0049] In a particular non-limiting, exemplary embodiment, the computer-readable medium can include a solid-state memory such as a memory card or other package that houses one or more non-volatile read-only memories. Further, the computer-readable medium can be a random access memory or other volatile re-writable memory. Additionally, the computer-readable medium can include a magneto-optical or optical medium, such as a disk or tapes or other storage device to capture carrier wave signals such as a signal communicated over a transmission medium. A digital file attachment to an e-mail or other self-contained information archive or set of archives may be considered a distribution medium that is a tangible storage medium. Accordingly, the disclosure is considered to include any one or more of a computer-readable medium or a distribution medium and other equivalents and successor media, in which data or instructions may be stored.

[0050] In an alternative embodiment, dedicated hardware implementations, such as application specific integrated circuits, programmable logic arrays and other hardware devices, can be constructed to implement one or more of the methods described herein. Applications that may include the apparatus and systems of various embodiments can broadly include a variety of electronic and computer systems. One or more embodiments described herein may implement functions using two or more specific interconnected hardware modules or devices with related control and data signals that can be communicated between and through the modules, or as portions of an application-specific integrated circuit. Accordingly, the present system encompasses software, firmware, and hardware implementations.

[0051] In accordance with various embodiments of the present disclosure, the methods described herein may be implemented by software programs executable by a computer system. Further, in an exemplary, non-limited embodiment, implementations can include distributed processing, component/object distributed processing, and parallel processing. Alternatively, virtual computer system processing can be constructed to implement one or more of the methods or functionality as described herein.

[0052] Although the present specification describes components and functions that may be implemented in particular embodiments with reference to particular standards and protocols, the invention is not limited to such standards and protocols. For example, standards for Internet and other packet switched network transmission (e.g., TCP/IP, UDP/IP, HTML, HTTP, HTTPS) represent examples of the state of the art. Such standards are periodically superseded by faster or more efficient equivalents having essentially the same functions. Accordingly, replacement standards and protocols having the same or similar functions as those disclosed herein are considered equivalents thereof.

[0053] A computer program (also known as a program, software, software application, script, or code) can be written in any form of programming language, including compiled or interpreted languages, and it can be deployed in any form,

including as a standalone program or as a module, component, subroutine, or other unit suitable for use in a computing environment. A computer program does not necessarily correspond to a file in a file system. A program can be stored in a portion of a file that holds other programs or data (e.g., one or more scripts stored in a markup language document), in a single file dedicated to the program in question, or in multiple coordinated files (e.g., files that store one or more modules, sub programs, or portions of code). A computer program can be deployed to be executed on one computer or on multiple computers that are located at one site or distributed across multiple sites and interconnected by a communication network.

[0054] The processes and logic flows described in this specification can be performed by one or more programmable processors executing one or more computer programs to perform functions by operating on input data and generating output. The processes and logic flows can also be performed by, and apparatus can also be implemented as, special purpose logic circuitry, e.g., an FPGA (field programmable gate array) or an ASIC (application specific integrated circuit).

[0055] Processors suitable for the execution of a computer program include, by way of example, both general and special purpose microprocessors, and anyone or more processors of any kind of digital computer. Generally, a processor will receive instructions and data from a read only memory or a random access memory or both. The essential elements of a computer are a processor for performing instructions and one or more memory devices for storing instructions and data. Generally, a computer will also include, or be operatively coupled to receive data from or transfer data to, or both, one or more mass storage devices for storing data, e.g., magnetic, magneto optical disks, or optical disks. However, a computer need not have such devices. Moreover, a computer can be embedded in another device, e.g., a mobile telephone, a personal digital assistant (PDA), a mobile audio player, a Global Positioning System (GPS) receiver, to name just a few. Computer readable media suitable for storing computer program instructions and data include all forms of non volatile memory, media and memory devices,

including by way of example semiconductor memory devices, e.g., EPROM, EEPROM, and flash memory devices; magnetic disks, e.g., internal hard disks or removable disks; magneto optical disks; and CD ROM and DVD-ROM disks. The processor and the memory can be supplemented by, or incorporated in, special purpose logic circuitry.

[0056] To provide for interaction with a user, embodiments of the subject matter described in this specification can be implemented on a device having a display, e.g., a CRT (cathode ray tube) or LCD (liquid crystal display) monitor, for displaying information to the user and a keyboard and a pointing device, e.g., a mouse or a trackball, by which the user can provide input to the computer. Other kinds of devices can be used to provide for interaction with a user as well; for example, feedback provided to the user can be any form of sensory feedback, e.g., visual feedback, auditory feedback, or tactile feedback; and input from the user can be received in any form, including acoustic, speech, or tactile input.

[0057] Embodiments of the subject matter described in this specification can be implemented in a computing system that includes a back end component, e.g., as a data server, or that includes a middleware component, e.g., an application server, or that includes a front end component, e.g., a client computer having a graphical user interface or a Web browser through which a user can interact with an implementation of the subject matter described in this specification, or any combination of one or more such back end, middleware, or front end components. The components of the system can be interconnected by any form or medium of digital data communication, e.g., a communication network. Examples of communication networks include a local area network ("LAN") and a wide area network ("WAN"), e.g., the Internet.

[0058] The computing system can include clients and servers. A client and server are generally remote from each other and typically interact through a communication network. The relationship of client and server arises by virtue of computer programs running on the respective computers and having a client-server relationship to each other.

[0059] The illustrations of the embodiments described herein are intended to provide a general understanding of the structure of the various embodiments. The illustrations are not intended to serve as a complete description of all of the elements and features of apparatus and systems that utilize the structures or methods described herein. Many other embodiments may be apparent to those of skill in the art upon reviewing the disclosure. Other embodiments may be utilized and derived from the disclosure, such that structural and logical substitutions and changes may be made without departing from the scope of the disclosure. Additionally, the illustrations are merely representational and may not be drawn to scale. Certain proportions within the illustrations may be exaggerated, while other proportions may be minimized. Accordingly, the disclosure and the figures are to be regarded as illustrative rather than restrictive.

[0060] While this specification contains many specifics, these should not be construed as limitations on the scope of the invention or of what may be claimed, but rather as descriptions of features specific to particular embodiments of the invention. Certain features that are described in this specification in the context of separate embodiments can also be implemented in combination in a single embodiment. Conversely, various features that are described in the context of a single embodiment can also be implemented in multiple embodiments separately or in any suitable sub-combination. Moreover, although features may be described above as acting in certain combinations and even initially claimed as such, one or more features from a claimed combination can in some cases be excised from the combination, and the claimed combination may be directed to a sub-combination or variation of a sub-combination.

[0061] Similarly, while operations are depicted in the drawings and described herein in a particular order, this should not be understood as requiring that such operations be performed in the particular order shown or in sequential order, or that all illustrated operations be performed, to achieve desirable results. In certain circumstances, multitasking and parallel processing may be advantageous. Moreover, the separation of various system components in the embodiments

described above should not be understood as requiring such separation in all embodiments, and it should be understood that the described program components and systems can generally be integrated together in a single software product or packaged into multiple software products.

[0062] One or more embodiments of the disclosure may be referred to herein, individually and/or collectively, by the term "invention" merely for convenience and without intending to voluntarily limit the scope of this application to any particular invention or inventive concept. Moreover, although specific embodiments have been illustrated and described herein, it should be appreciated that any subsequent arrangement designed to achieve the same or similar purpose may be substituted for the specific embodiments shown. This disclosure is intended to cover any and all subsequent adaptations or variations of various embodiments. Combinations of the above embodiments, and other embodiments not specifically described herein, will be apparent to those of skill in the art upon reviewing the description.

[0063] The Abstract of the Disclosure is provided to comply with 37 C.F.R. §1.72(b) and is submitted with the understanding that it will not be used to interpret or limit the scope or meaning of the claims. In addition, in the foregoing Detailed Description, various features may be grouped together or described in a single embodiment for the purpose of streamlining the disclosure. This disclosure is not to be interpreted as reflecting an intention that the claimed embodiments require more features than are expressly recited in each claim. Rather, as the following claims reflect, inventive subject matter may be directed to less than all of the features of any of the disclosed embodiments. Thus, the following claims are incorporated into the Detailed Description, with each claim standing on its own as defining separately claimed subject matter.

[0064] It is therefore intended that the foregoing detailed description be regarded as illustrative rather than limiting, and that it be understood that it is the following claims, including all equivalents, that are intended to define the spirit and scope of this invention.

WHAT IS CLAIMED IS:

1. A programmable logic controller ("PLC") 100 comprising:

a communications interface 104 operative to communicate data between the PLC 100 and a device external thereto;

an attribute 106 characterized by a value unique to the PLC 100; and

an encryption processor 108 coupled between the attribute 106 and the communications interface 104 and operative to generate an encryption key unique to the PLC 100 based at least on the unique value of the attribute 106 and communicate the encryption key via the communications interface 104.

2. The PLC 100 of claim 1 further comprising:

a housing 102 in which at least the attribute 106 and encryption processor 108 are located, the communications interface 104 being further operative to communicate data through the housing 102.

3. The PLC 100 of claim 1 wherein the attribute 106 comprises a memory 116 having stored therein the unique value assigned to the PLC 100.

4. The PLC 100 of claim 1 comprising a physical characteristic unique to the PLC 100, the attribute comprising a generator 118 operative to generate the unique value as a function of the unique physical characteristic.

5. The PLC 100 of claim 1 wherein encryption key comprises a public encryption key of a key pair, the encryption processor 108 being further operative to generate a private encryption key of the key pair associated with the public encryption key based at least on the attribute, the private encryption key being stored in a memory 110 coupled with the encryption processor 108 internal to the PLC 100.

6. The PLC 100 of claim 1 further comprising a memory 110 internal to the PLC 100 coupled with the encryption processor 108 wherein the encryption processor 108 is further operative to store the encryption key in the memory.

7. The PLC 100 of claim 1 wherein the encryption processor 108 is further operative to encrypt communications to be transmitted via the communication interface 104 using the encryption key, decrypt communications received thereby using the encryption key, or combinations thereof.

8. The PLC of claim 1 further comprising a processor 112 coupled with the communications interface 104 wherein the processor 112 is operative to receive executable program code to be executed thereby via the communications interface 104, store the received executable program code in a memory 110 coupled therewith and validate the stored received executable program code using the encryption key before execution thereof by the processor 112.

9. The PLC of claim 1 wherein the encryption processor 108 is further operative to generate the encryption key in response to a request received thereby via the communications interface 104.

10. A computer implemented method for facilitating secure integrity of a programmable logic controller ("PLC") 100, the method comprising:

receiving, by a processor 108, a value of an attribute 106 unique to the PLC 100 which is not communicated via a communications interface 104 of the PLC 100 operative to communicate data between the PLC 100 and a device external thereto [block 202];

generating, by the processor 108, an encryption key unique to the PLC 100 based at least in part on the unique value [block 204]; and

communicating, by the processor 100, the encryption key via the communications interface 104 [block 206].

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

enclosing the processor 108 within a housing 102 in which at least the attribute 106 is located, the communications interface 104 being further operative to communicate data through the housing 102 [block 208].

12. The computer implemented method of claim 10 further comprising storing the unique value of the attribute 106 in a memory 116 coupled with the processor 108 [block 210].

13. The computer implemented method of claim 10 wherein the PLC 100 is further characterized by a physical characteristic unique to the PLC 100, the method further comprising generating the unique value as a function of the unique physical characteristic [block 212].

14. The computer implemented method of claim 10 wherein the encryption key comprises a public encryption key of a key pair , the method further comprising:

generating a private encryption key of the key pair associated with the public encryption key based at least on the unique value [block 214]; and

storing the private key in a memory 110 coupled with the processor 108 [block 216].

15. The computer implemented method of claim 10 further comprising storing, by the processor, the encryption key in a memory 110 internal to the PLC 100 and coupled with the processor 108 [block 218].

16. The computer implemented method of claim 10 further comprising:

encrypting, by the processor 108 communications to be transmitted by the communications interface 104 using the encryption key [block 220];

or

decrypting, by the processor 108, communications received by the communications interface 104 using the encryption key [block 222].

17. The computer implemented method of claim 10 further comprising:

receiving, by the processor 108 via the communications interface 104, executable computer program code for execution by the PLC 100 [block 224];

storing, by the processor 108, the received executable computer program code in a memory 110 coupled therewith [block 226];

validating, by the processor 108, the received executable computer program code based on the encryption key [block 228]; and

executing the stored received executable computer program code only if validated [block 230].

18. The computer implemented method of claim 10 further comprising:

receiving, by the processor 108 via the communications interface 104, a request to generate the encryption key [block 232]; and

wherein the generating further comprises generating the encryption key responsive to the request [block 204].

19. A system for facilitating secure integrity of a programmable logic controller ("PLC") 100, the system comprising:

means for receiving a value of an attribute unique to the PLC 100 which is not communicated via a communications interface 104 of the PLC 100 operative to communicate data between the PLC 100 and a device external thereto;

means for generating an encryption key unique to the PLC 100 based at least in part on the unique value; and

means for communicating the encryption key via the communications interface 104.

20. The system of claim 19 further comprising:

means for housing the receiving means and generating means and wherein the means for communicating further enable communications through the housing means.

FIG. 1

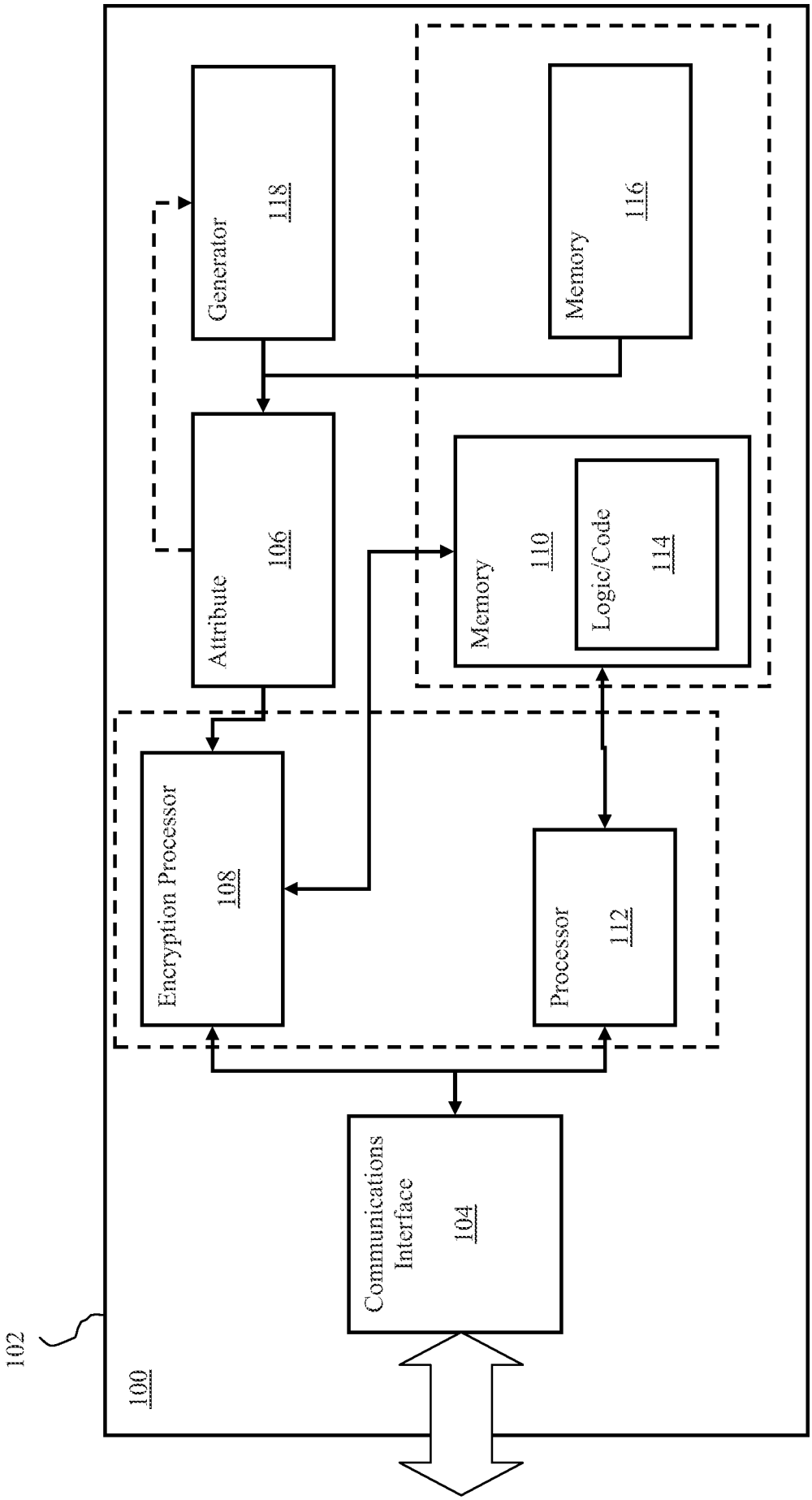

Generator 118
Memory 116
Attribute 106
Memory 110
Logic/Code 114
Encryption Processor 108
Processor 112
Communications Interface 104
102
100

FIG. 2

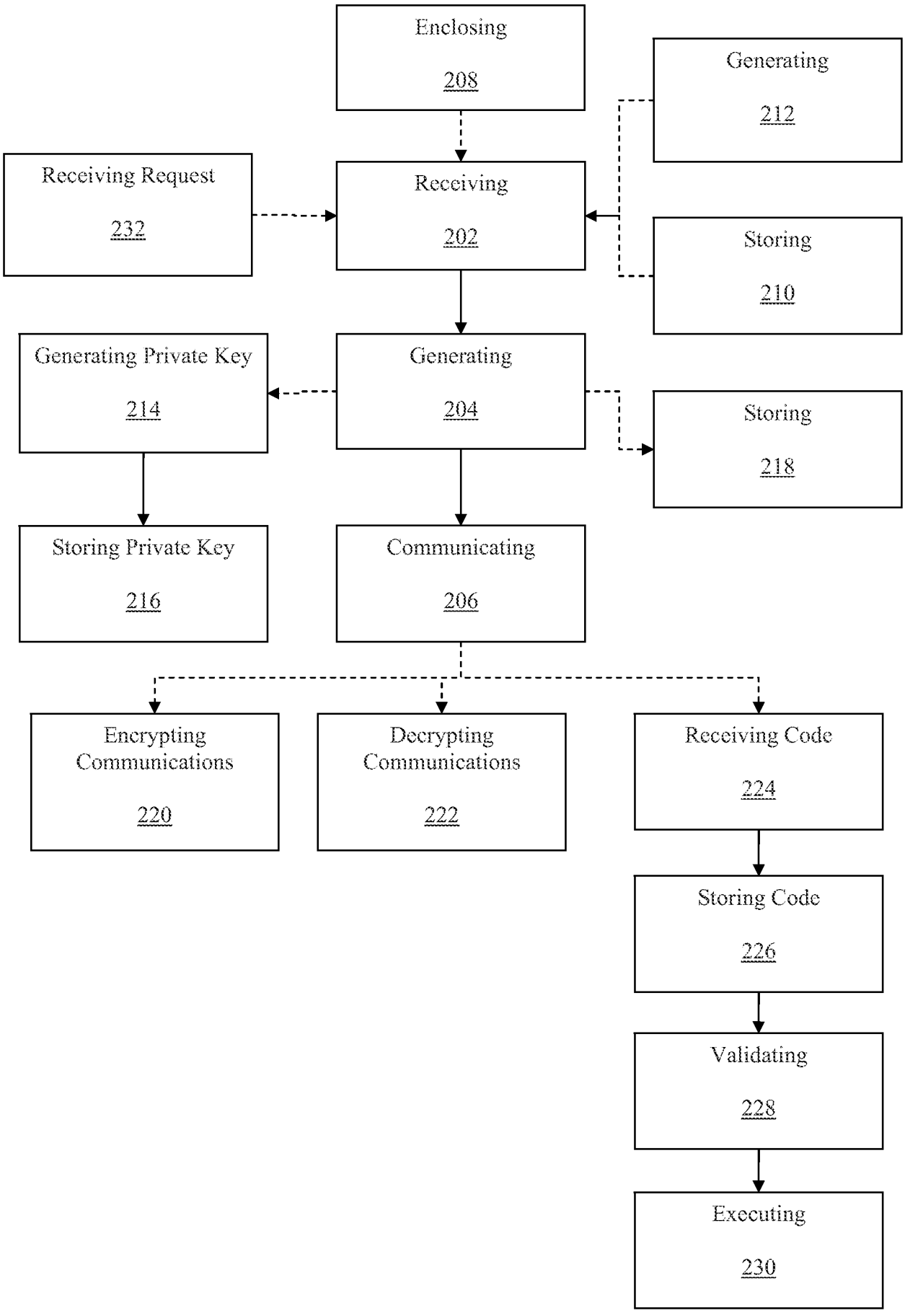

Enclosing
208
Generating
212
Receiving Request
232
Receiving
202
Storing
210
Generating Private Key
214
Generating
204
Storing
218
Storing Private Key
216
Communicating
206
Encrypting Communications
220
Decrypting Communications
222
Receiving Code
224
Storing Code
226
Validating
228
Executing
230

FIG. 3

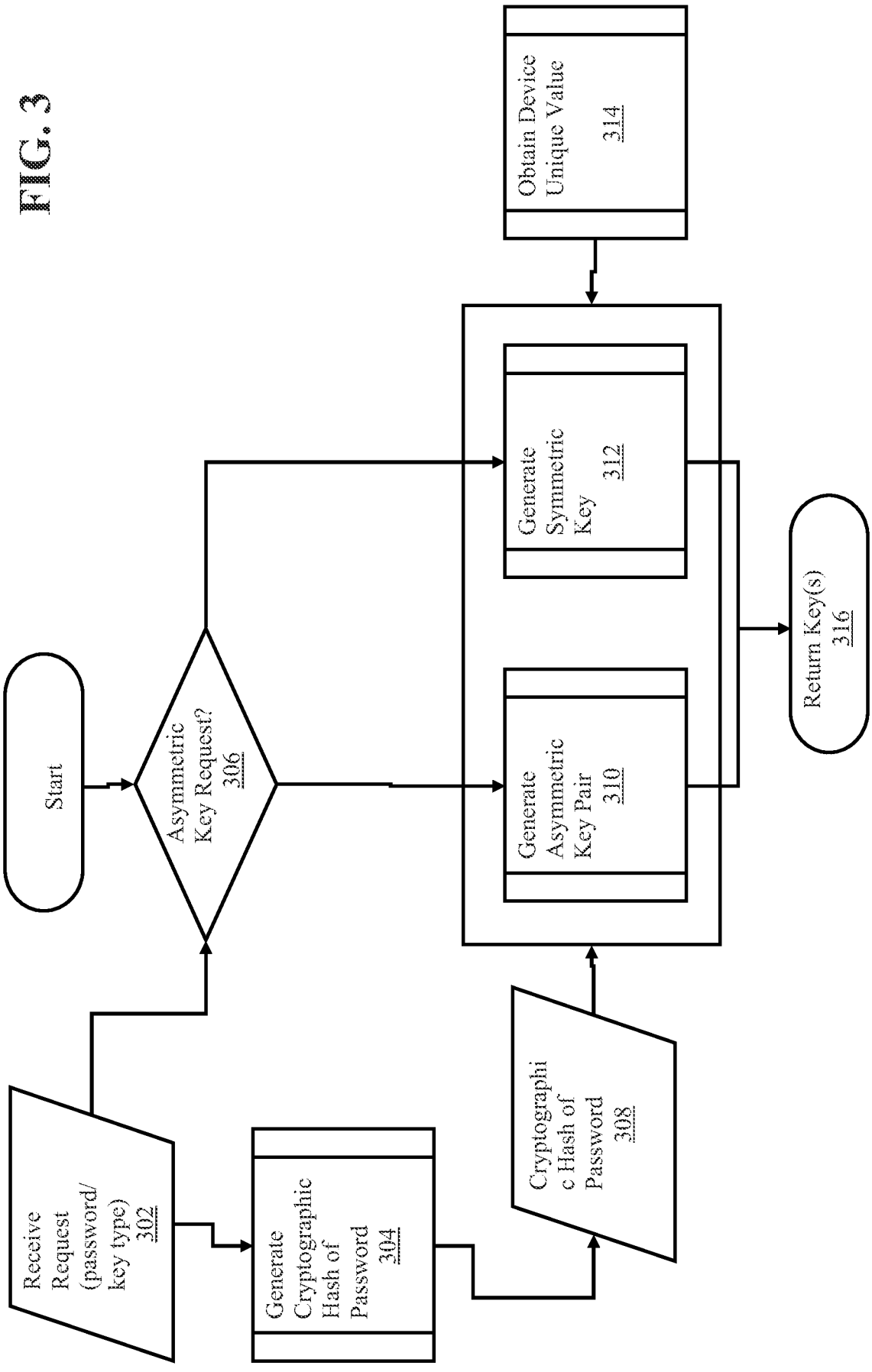
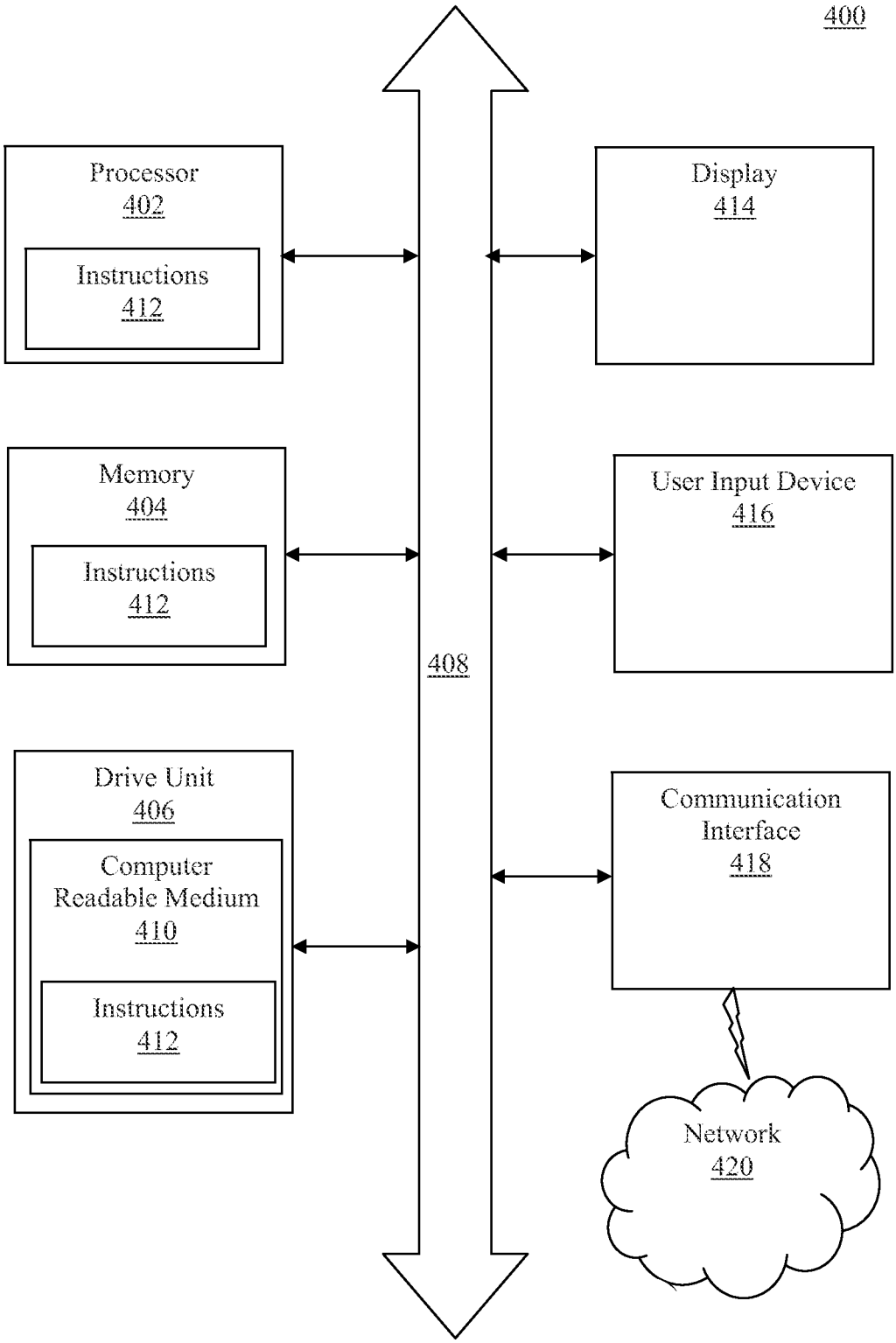

Start
Receive Request (password/ key type) 302
Asymmetric Key Request? 306
Generate Cryptographic Hash of Password 304
Cryptographic Hash of Password 308
Generate Asymmetric Key Pair 310
Generate Symmetric Key 312
Obtain Device Unique Value 314
Return Key(s) 316

FIG. 4


400
Processor
402
Instructions
412
Display
414
Memory
404
Instructions
412
User Input Device
416
408
Drive Unit
406
Computer
Readable Medium
410
Instructions
412
Communication
Interface
418
Network
420

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2012/030516

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/08 H04L9/32 G06F21/62
ADD.

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L G06F

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 7 191 339 B1 (TRIMBERGER STEPHEN M [US]) 13 March 2007 (2007-03-13) abstract; claims 1,2,11-13; figures 1,2,5-7 column 1, line 12 - line 18 column 1, line 44 - column 2, line 42 column 2, line 61 - last line column 3, line 66 - column 4, line 39 column 6, line 50 - column 7, line 30 -----	1-20
X	EP 2 006 792 A2 (SIEMENS AG [DE]) 24 December 2008 (2008-12-24) abstract; claims 1-5,8,10,11; figures 1,2 paragraphs [0002], [0003], [0008] - [0015], [0021] - [0023], [0027] paragraphs [0030] - [0040], [0044] - [0046], [0048] - [0053] ----- -/--	1-20

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
4 December 2012	11/12/2012

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Wolters, Robert

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2012/030516

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 1 582 950 A2 (ROCKWELL AUTOMATION TECH INC [US]) 5 October 2005 (2005-10-05) abstract; claims 1,3-8,11,12; figures 1,3,5 paragraphs [0004], [0005], [0007], [0008], [0023], [0024], [0028] -----	1-20
Y	WO 2012/016858 A1 (SIEMENS AG [DE]; BUSSER JENS-UWE [DE]; FRIES STEFFEN [DE]) 9 February 2012 (2012-02-09) abstract; claims 1-5,11,12 page 2, line 33 - page 3, line 30 -----	1-20

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2012/030516

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 7191339 B1	13-03-2007	NONE	
EP 2006792 A2	24-12-2008	CN 101329658 A	24-12-2008
		EP 2006792 A2	24-12-2008
EP 1582950 A2	05-10-2005	EP 1582950 A2	05-10-2005
		US 2005229004 A1	13-10-2005
		US 2010077217 A1	25-03-2010
WO 2012016858 A1	09-02-2012	DE 102010033232 A1	09-02-2012
		WO 2012016858 A1	09-02-2012