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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 March 2018 (15.03.2018)

WIPO | PCT

(10) International Publication Number
WO 2018/045475 A1

(51) International Patent Classification:
H04L 9/32 (2006.01) *H04L 9/30* (2006.01)
H04L 9/08 (2006.01)

(21) International Application Number:
PCT/CA2017/051067

(22) International Filing Date:
11 September 2017 (11.09.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/393,549 12 September 2016 (12.09.2016) US

(71) Applicant: **NANOPORT TECHNOLOGY INC.** [CA/CA]; 75 Springfield Drive, Markham, Ontario L3S 3H5 (CA).

(72) Inventors: **SZETO, Timothy Jing Yin**; 510-3939 Duke of York Boulevard, Mississauga, Ontario L5B 4N2 (CA). **REYES, David Michael Lopez**; 97 Old Finch Avenue, Toronto, Ontario M1B 5G5 (CA). **BARAKE, Omar George Jospeh**; 537 Fox Cove Place, Waterloo, Ontario N2K 4C6 (CA).

(74) Agent: **NORTON ROSE FULBRIGHT CANADA LLP**; 1, Place Ville Marie, Suite 2500, Montreal, Québec H3B 1R1 (CA).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, 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, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

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

(54) Title: SECURE INDIRECT ACCESS PROVISIONING OF OFF-LINE UNPOWERED DEVICES BY CENTRALIZED AUTHORITY

(57) Abstract: Embodiments described herein relate to systems and processes for provisioning access to resources of electronic devices. The systems and processes can involve a centralized authority connected to a first device which is in turn connected to a second device. The first device transmits an access request to the centralized authority. The access request requests access by the first device to the one or more resources of the second device using a connection link between the first device and the second device. The centralized authority is configured to process the access request by verifying the access request against access right records. The centralized authority is configured to generate a response to the access request that includes instructions to instruct the second device to allow the first device to access the one or more resources using the connection link. The response is encoded to be not readable by the first device and readable by the second device.

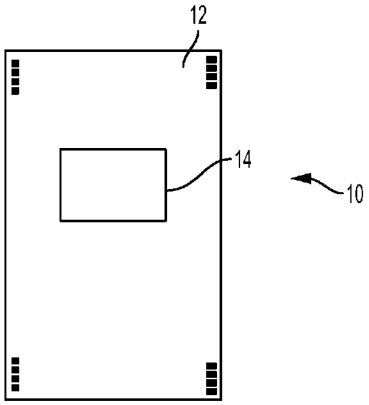

FIG. 1

WO 2018/045475 A1

TITLE: SECURE INDIRECT ACCESS PROVISIONING OF OFF-LINE UNPOWERED DEVICES BY CENTRALIZED AUTHORITY

FIELD

[0001] The embodiments generally relate to the field of electronic devices and provisioning access to resources of electronic devices.

INTRODUCTION

[0002] Electronic devices may have one or more resources that can be accessed by other electronic devices. Example resources may include, e.g., memory, battery power, actuators, sensors, and so on.

SUMMARY

[0003] In accordance with an aspect, there is provided a centralized server for provisioning access to resources. The server can include a persistent data repository storing access right records including a first access right record with a first access right of a first device to one or more resources of a second device. The server can include a processor configured to receive a first access request from the first device, the first access request requesting access by the first device to the one or more resources of the second device using a connection link between the first device and the second device; process the first access request by verifying the first access request against the access right records; generate a first response to the first access request, the first response comprising a message for the first device to relay to the second device, the message comprising instructions to instruct the second device to allow the first device to access the one or more resources using the connection link, the first message encoded to be not readable by the first device and readable by the second device; and transmit the first response.

[0004] In some embodiments, the processor is configured to transmit the first response to the second device by transmitting the message to the first device for relay to the second device.

[0005] In some embodiments, the persistent data repository stores a public key for the second device. The processor can be configured to generate the first response by encrypting at least a portion of the response comprising the message using the public key for the second device, the at least a portion of the first response for decryption by the second device using a corresponding private key for the second device.

[0006] In some embodiments, the persistent data repository stores a server private key, the processor being configured to generate the response by encrypting at least the portion of the response using the server private key for decryption by the second device using a corresponding server public key.

[0007] In some embodiments, the message comprises a device identifier for the first device.

[0008] In some embodiments, the message is a first message and the first response further comprises a second message for the first device.

[0009] In some embodiments, the persistent data repository stores a public key for the first device, the processor being configured to generate the first response by encrypting at least a portion of the response comprising the second message using the public key for the first device, the at least a portion of the first response for decryption by the first device using a corresponding private key.

[0010] In some embodiments, the processor can be configured to generate a symmetric key, wherein the first message comprises the symmetric key for the first and second devices to establish a secured communication link.

[0011] In some embodiments, the second message comprises the symmetric key.

[0012] In some embodiments, the persistent data repository can link a first device identifier and the first access right record, the first access request indicating a first device identifier, and the processor being further configured to process the first access request by verifying the first device identifier.

[0013] In some embodiments, the persistent data repository can store user profiles including a first user profile linking a first user identifier, the second device and the first access right record, the first access request indicating the first user identifier, wherein the processor is configured to process the first access request using the first user profile to locate the first access right record.

[0014] In some embodiments, the first response includes an access time period having a start time and an end time, wherein the processor is configured to generate the message comprising instructions to instruct the second device to allow the first device to access the one or more resources only during the access time period.

[0015] In some embodiments, the first access right is selected from the group of an access right to establish a connection link to the second device, an access right to write data to a memory resource of the second device, an access right to read data from a memory resource of the second device, an access right to transfer data to and from a memory resource of the second device, an access right to transfer and process data using a processing resource of the second device, an access right to display data using a display device resource of the second device, an access right to receive data from an input device resource of the second device, an access right to capture data using a sensor resource of the second device, and an access right to activate an actuator resource of the second device.

[0016] In some embodiments, the first access request can identify the connection link of the one or more connectors between the first device and the second device.

[0017] In some embodiments, the centralized server can be in communication with the first device but not in communication with the second device.

[0018] In some embodiments, the persistent data repository can store a first public key in association with the first device, a second public key in association with the second device, and a server private key. The processor can be configured to generate the first response by: generating a symmetric key for the first device and the second device to establish a secure communication channel for inclusion in the first message and the second message; encrypting at least a portion of the response comprising the message with the second public key and the server private key; and encrypting at least a portion of the response with the first public key and the server private key.

[0019] In some embodiments, the persistent data repository is configured to store a second access right record with a second access right of the first device to one or more resources of a third device. The processor can be further configured to receive a second access request from the first device, the second access request requesting access by the first device to the one or more resources of the third device using a second connection link between the first device and the third device; process the second access request by verifying the second access request against the access right records; generate a second response to the second access request, the second response comprising a second message for the first device to relay to the third device, the second message comprising instructions to instruct the third device to allow the first device to access the one or more resources using the connection link, the first message

encoded to be not readable by the first device and readable by the third device; and transmit the second response.

[0020] In some embodiments, the processor can be configured to receive a third access request from the first device, the third access request requesting access by the first device to an additional resource of the second device using the connection link; process the third access request by verifying the third access request against the access right records; generate a third response to the third access request, the response denying the third access request; and transmit the third response.

[0021] In some embodiments, the processor can be configured to authenticate the first device by verifying a first user identifier or a first device identifier against the access right records.

[0022] In some embodiments, the first access right record includes a first device identifier, a second device identifier and a resource identifier, the first access request comprising the first device identifier, the second device identifier and the resource identifier. The processor is configured to process the first access request by verifying the access request against the access right records using the first device identifier, the second device identifier and the resource identifier.

[0023] In another aspect, there is provided a process for provisioning access to resources using a centralized server. The process can involve: transmitting, by a first device, an access request from to the centralized server, the access request requesting access to one or more resources of a second device by the first device using a connection link between the first device and the second device; receiving a response to the access request from the centralized server, the response comprising a first portion for the first device to relay to the second device and encoded to be not readable by the first device and readable by the second device; decrypting at least a second portion of the response using a private key of the first device and a public key of the centralized server; transmitting the first portion of the response to the second device using the connection link; and accessing, by the first device, the one or more resources of the second device using the connection link.

[0024] In some embodiments, the process can involve receiving a second device identifier; and transmitting the second device identifier with the access request.

[0025] In some embodiments, the process can involve providing power from the first device to the second device in order to access the one or more resources or transmit the portion of the response.

[0026] In some embodiments, the process can involve receiving a symmetric key from the centralized server; transmitting the symmetric key to the second device as part of the first portion of the response; and transmitting data encrypted using the symmetric key to the second device.

[0027] In another aspect, there is provided a device for requesting access to resources using a centralized server. The device can include a communication interface to establish a connection link to a second device having one or more resources. The device can include a processor configured to: transmit an access request to the centralized server, the access request requesting access to the one or more resources of the second device using the connection link; receive a response to the access request from the centralized server, the first response comprising a portion for the first device to relay to the second device, the portion of the first response comprising instructions to instruct the second device to allow the first device to access the one or more resources using the connection link, the portion of the first response encoded to be not readable by the first device and readable by the second device; transmit the portion of the first response to the second device using the connection link; and access the one or more resources of the second device using the connection link.

[0028] In some embodiments, the processor is configured to receive a second device identifier and from the second device and transmit the second device identifier with the access request.

[0029] In some embodiments, the device can include a power supply wherein the processor is configured to transfer power from the power supply to the second device.

[0030] Many further features and combinations thereof concerning embodiments described herein will appear to those skilled in the art following a reading of the instant disclosure.

DESCRIPTION OF THE FIGURES

[0031] Embodiments will now be described, by way of example only, with reference to the attached figures, wherein in the figures:

[0032] FIG. 1 is diagram of a device according to some embodiments;

[0033] FIG. 2 is diagram of two devices according to some embodiments;

[0034] FIG. 3 is diagram of a system for provisioning access to resources of one or more electronic devices according to some embodiments;

[0035] FIG. 4A is diagram of access right records according to some embodiments;

[0036] FIG. 4B is diagram of access right records according to some embodiments;

[0037] FIG. 5 is diagram of a system for provisioning access to resources of one or more electronic devices according to some embodiments;

[0038] FIG. 6 is workflow diagram of a process for provisioning access to resources of one or more electronic devices according to some embodiments;

[0039] FIG. 7 is workflow diagram of a process for provisioning access to resources of one or more electronic devices according to some embodiments;

[0040] FIG. 8 is workflow diagram of a process for provisioning access to resources of one or more electronic devices according to some embodiments; and

[0041] FIG. 9 is workflow diagram of a process for provisioning access to resources of one or more electronic devices according to some embodiments;

DETAILED DESCRIPTION

[0042] Embodiments described herein relate to systems and methods for provisioning access to resources of a device to an interconnected device, using a centralized authority.

[0043] **FIG. 1** is a diagram of a device 10 according to some embodiments. Device 10 may be configured to function as a smartphone, and thus may include various smartphone components. For example, device 10 may include electronics 14 incorporating a suitable combination of processors, memory, I/O interfaces (e.g., wireless interfaces for connection to

the Internet). Device 10 may also have other smartphone components such as a display, touchscreen, sensors, etc., which are omitted for clarity of illustration. Device 10 is configured to request access to one or more resources of another device 10 using a centralized authority, according to some embodiments. In some embodiments, device 10 is configured to grant access to its resources by another device.

[0044] Device 10 can include magnetic connectors 12 for connecting to other devices 10. Magnetic connectors 12 and examples of devices 10 incorporating such connectors 12 are described in International Application No. PCT/CA2014/000803 and U.S. Patent No. 9312633, the contents of each of which are incorporated by reference. Such connectors are herein referred to as Nanoport connectors 12 for convenience. Nanoport connectors 12 can provide a mechanical connection between two or more devices. A Nanoport connector 12 may additionally transmit data and/or power between the devices 10. In some embodiments, device 10 includes Nanoport connectors 12 at its corners.

[0045] Devices 10 may have various other form factors (e.g., smart watch, tablet devices, etc.), and have fewer or a Nanoport connectors 12, arranged at various locations on the device 10. By way of example, **FIG. 2** is a diagram that illustrates two devices 10 having different form factors and Nanoport connectors 12 arranged at various locations.

[0046] Nanoport connectors 12 may be included in a variety of devices 10, such as, e.g., peripheral devices (electronic storage devices such as portable hard drives, or batteries, keyboards, speakers, etc.), household appliances, vehicles, consumer electronic devices, industrial machinery, etc. Such devices 10 may be configured with suitable electronics and logic for establishing a data link and/or a power link with another device 10, e.g., through a Nanoport connector 12. In some cases, a device 10 may be substantially similar to the other connected device 10, such as a smartphone, smartwatch, or similar device. In some cases, the device 10 may be different from to the other connected device 10.

[0047] Each device 10 may have one or more resources that can be provisioned to another device 10. Such resources may include, e.g., memory, battery power, actuators, sensors, etc. Data and/or power associated with accessing such resources may be transferred to another device 10 by way of Nanoport connectors 12 in some embodiments.

[0048] **FIG. 3** is a schematic diagram of a system for provisioning access to resources according to some embodiments. The system can include centralized authority 200 and devices 100. The devices 100 may generally correspond to the devices 10 of **FIGS. 1** and **2**.

[0049] As shown, the centralized authority 200 can connect to one or more devices 100, e.g., by way of a network such as the Internet or an intranet. In some embodiments, the centralized authority 200 connects to one of the devices 100, or a subset of the devices 100. A first device 100 connects to a second device 100 by way of a connection link. The connection link can involve Nanoport connectors 12, as shown in **FIGS. 1** and **2**, for example. The connection link can be a wired or wireless connection link, for example.

[0050] Access to specific resources of devices 100 may be governed by the centralized authority 200, e.g., at a remote server. Centralized authority 200 includes at least one persistent data store 202 and at least one processor 204. The persistent data store 202 includes instructs and rules to control and command the at least one processor 204.

[0051] The centralized authority 200 is configured to provision access by a device 100 to resources of one or more other devices 100. The centralized authority 200 can include a persistent data repository (e.g. as part of the at least one persistent data store 202) with a database 300 storing access right records. The access right records can include a first access right record with a first access right to permit a first device 100 to access one or more resources of a second device 100. Database 300 may be relational, object-oriented, graph and so on. Database 300 may store access right records reflective of devices 100 associated with particular users or user profiles. A user may have multiple profiles, suitable for different operating scenarios (e.g., home/personal, work, private/incognito). The access right records may store data reflective of access rights to particular resources at particular devices 100. For example, access rights may include rights to connect to particular devices 100, rights to read from particular sensors at particular devices 100, rights to activate particular actuators at particular devices 100, and so on. Access rights may be circumscribed in time, with defined start times and stop times or an activation time period, for example. Access rights may be user-defined, e.g., by the owners of the respective devices. Access rights may be defined by an administrator or organization, e.g., by employers associated with the respective devices.

[0052] **FIG. 4A** shows an example data structure 400 that includes user profiles 402, devices associated with those user profiles, and access rights for those devices under those

user profiles 402. Each access right defines the right of one or more users associated with a particular user profile 402 to access particular resources at a particular device. One user may be associated with multiple user profiles 402 in some embodiments (e.g., a work profile and a home profile). A user profile 402 may be associated with multiple users in some embodiments (e.g., when multiple users such as in a family share the same access rights). A user profile 402 can be associated with multiple devices 100 to define access rights for each of those devices 100 in some embodiments. Multiple user profiles 402 can be associated with the same or different devices 100. The user profiles 402 can be respectively associated with, respectively, different users in some embodiments. A user profile 402 can be linked to a user by way of a unique user identifier or token, for example. The user profile 402 can be linked to different devices 100 by way of a device identifier, for example. A device 100 may be linked to different access rights for different user profiles 402. An access right can define the scope of permitted access by a device 100 which can include one or more resources, one or more operations, and so on. In some embodiments, user profiles may be omitted, and access right records may be associated with particular users rather than user profiles. For example, an access right record may be linked directly to a user identifier instead of to a user profile. As another example, an access right record may be linked directly to a device identifier, which may in turn be linked to a user identifier.

[0053] **FIG. 4B** shows another example data structure 410 that includes device profiles 412 and access rights linked to the devices profiles 412. In this example, data structure 410 includes a plurality of device profiles 412, which may be uniquely associated with a device (e.g., by way of a unique device ID). Each device profile 412 defines access rights to its associated device, e.g., which may grant access to particular resources of that device to particular users, particular user profiles, particular classes of users, particular other devices, and so on.

[0054] Centralized authority 200 is configured to receive access requests from a first device 100 for resources of a particular second device 100. Centralized authority 200 is configured to respond (e.g., permit or deny) to such requests by verifying the access request against stored access right records.

[0055] In some embodiments, the centralized authority 200 has a processor configured to receive a first access request from the first device 100. The first access request is a data structure or electronic message that requests access by the first device 100 to the one or more resources of the second device 100. The access request can identify the first device 100, the

second device 100, the one or more resources of the second device 100, the user, a time period for the request, and other information that may be relevant to the request. If the access request is granted, the first device 100 can then access the resources of the second device 100 using a connection link between the first device 100 and the second device 100.

[0056] The processor is further configured to process the first access request by verifying the first access request against the access right records. The processor can verify the access request in different ways. For example, the processor can compare data within the access request against data within the access right records to confirm or deny the access request. The processor can determine a user identifier associated with the first access request and retrieve one or more user profiles 402 linked to that user identifier. The processor can also determine a profile identifier associated with the first access request in the event the user is linked to multiple user profiles 402. The profile identifier can be used to determine a particular user profile 402 of the multiple user profiles 402 linked to the particular user. The processor can determine a device identifier associated with the second device 100 to determine access rights linked to the first device 100 and the second device 100 within the user profile 402. As another example, the access request may be encrypted at first device 100 using a key associated with the first device 100. The processor is configured to decrypt the encrypted access request using a corresponding key. If the decryption is successful this may be used to verify the access request by confirming that the access request is associated with the first device 10 as only a corresponding key can be used by the processor to decrypt the access request.

[0057] The processor is further configured to generate a first response to the first access request. The first response includes a message for the first device 100 to relay to the second device 100. The message can include instructions to instruct the second device 100 to allow the first device 100 to access the one or more resources using the connection link. The message can also include instructions to instruct the second device 100 to deny the first device 100 with access to the one or more resources. In some example embodiments, the first message is encoded or encrypted by the processor to be not readable by the first device and readable by the second device. This may enhance security as a first device 100 is not able to read or tamper with the message. This may be helpful if the message denies the first access request and does not permit access by the first device 100 to the one or more resources of the second device 100.

[0058] The processor is further configured to transmit the first response. The processor can transmit the first response to the first device 100. The first device 100 can then relay the response to the second device 100 to instruct the second device 100 to allow or deny the first device 100 with access to the one or more resources. In some embodiments the processor can transmit the first response to the second device 100 directly.

[0059] In some example embodiments, the centralized authority 200 includes a persistent data repository that stores a public key for the first device 100. The processor is configured to use this public key to decrypt at least a portion of the access request which is encrypted by first device 100 using a corresponding private key. In some example embodiments, the centralized authority 200 includes a persistent data repository that stores a public key for the second device 100. The processor is configured to generate the first response by encrypting at least a portion of the response with the message using the public key for the second device 100. The portion of the first response being for decryption by the second device 100 using a corresponding private key. Other encryption and security techniques can be used.

[0060] In one example, the first and second devices 100 are both connected to the Internet or other network and both may communicate with centralized authority 200. The first device 100 and second device 100 may be connected to each other through Nanoport connectors 12 or another connection link. A user operating the first device 100 may desire to access resources at the second device 100 for one or more operations. An example of accessing resources includes reading a memory at a second device 100 and transferring data therefrom. Another example of accessing resources includes transferring data to a second device 100 and writing the data to a memory of the second device 100. A further example includes transferring data to a second device and displaying a visualization of the data at a display of the second device 100. These are illustrative examples.

[0061] In this example, the first device 100 transmits to the centralized authority 200 an access request to access the desired memory resource at the second device 100. The access request includes a device identifier of the second device 100 and the particular resource being requested. The access request can also identify the first device 100 or a user or a user profile associated with the first device 100. The access request includes or is accompanied by the credentials of the user associated with the first device 100. Optionally, the credentials may be associated with a particular user profile that is in turn linked to the user or the device 100.

[0062] Centralized authority 200 verifies the credentials of the user or user profile. For example, that the centralized authority may receive credentials that include a username and password that it compares to stored usernames and passwords for verification. The credentials can also include a secure token linked to the user or the first device 100, for example. Centralized authority 200 then processes the request by verifying that the user (or user profile) has access rights (as reflected in the access right records 402 of database 300) for the requested resource of the second device 100.

[0063] Upon successful verification, centralized authority 200 transmits a response to the access request to the second device 100, e.g., to instruct second device 100 to allow first device 100 to access the requested resource, e.g., by way of data/power transfer through Nanoport connectors 12.

[0064] In another example, the first device 100 is connected to the Internet or other network but the second device 100 is not. In this situation, only the first device 100 is able to communicate with centralized authority 200. The first device 100 may still transmit an access request for resources to centralized authority 200, but the centralized authority 200 is unable transmit a response directly to the second device 100. Instead, centralized authority 200 transmits the response to the first device 100 for relay to the second device 100.

[0065] In this example situation, at least two problems can arise. First, the second device 100 needs to verify that a response relayed through the first device 100 was from centralized authority 200, and was not spoofed or altered by the first device 100, for example. Second, the response to be relayed to the second device 100 should not be readable by the first device 100. For example, this may be desirable so that device 10 does not decline to relay a response because it is unfavourable, e.g., if the response not only denies the first device's 100 request but takes away the first device's 100 access to other (e.g., previously approved) resources.

[0066] Embodiments described herein may provide a system that includes public-key cryptography, namely, a cryptographic system that uses pairs of keys: public keys that may be disseminated paired with private keys which are known only to one holder. In particular, embodiments described herein may involve using a public key to authenticate that a message originated with a holder of the paired private key. As another example, embodiments described herein may involve encrypting a message with a public key to ensure that only the holder of the paired private key can decrypt it.

[0067] **FIG. 5** depicts such an example system 500 that uses cryptography to secure messages relating to access requests.

[0068] The centralized authority 200 connects to devices 100 in various ways including directly coupled and indirectly coupled via a network. The network can involve wired connections, wireless connections, or a combination thereof.

[0069] The centralized authority 200 is configured to receive on access request 506 from a first device 100. The centralized authority 200 is configured to process the access request 506 using the access right records. The centralized authority is configured to generate a response 518 to the access request 506, which may allow access to some or all of the requested resources (i.e., a positive response) or deny access to the requested resources (e.g., a negative response). In some embodiments, the centralized authority 200 is configured to generate a message 508 for the first device 100 and a message 510 for a second device 100. The message 510 for the second device 100 can include the response 518. The message 510 (including the response 518) for the second device 100 may not be readable by the first device 100. The first device 100 can relay the message 510 to the second device 100.

[0070] The centralized authority 200 maintains a database 300 of public keys 502 for devices 100. The centralized authority 200 is configured to link each public key 502 to a particular device 100 using data record that associates the public key 502 (or an identifier or reference for the public key 502) with a unique identifier for the device 100. The centralized authority 200 is configured to encode or encrypt messages 508, 510 for a particular device 100 using its corresponding public key 502. The centralized authority 200 maintains its own private key 504. The centralized authority 200 is configured to encode or encrypt messages 508, 510 that it generates using its private key 504. The devices 100 store or access a public key 512, 530 for the centralized authority 200 in order to decrypt messages that are encoded or encrypted using the private key 504 for the centralized authority 200. The use of the private key 504 and the corresponding public key 512, 530 provides a mechanism to verify that the centralized authority 200 created or sent a particular message 508, 510. The use of a public key 502 for the device 100 and a corresponding private key 512, 530 provides a mechanism to secure a particular message 508, 510 to be readable only by a particular device 100. In some example embodiments, the centralized authority 200 retrieves or generates a symmetric key 516. The centralized authority 200 is configured to generate a message 508, 510 that includes the symmetric key 516, which may be generated at the centralized authority 200. The first

device 100 and the second device 100 can create a secure communication channel using the symmetric key 516. The symmetric key may be generated to be unique for a particular session, unique for a particular pair of devices, unique for a particular user of the second device 100, unique for a particular class of users of the second device 100, or unique for a particular set of resources for which access is granted. In some embodiments, the centralized authority 200 may store symmetric keys within database 300, e.g., for subsequent transmission to another user in the same user class.

[0071] In some embodiments, a first device 100 may connect directly to the centralized authority 200. The first device 100 may wish to access one or more resources of the second device 100. The second device 100 may connect to the first device 100 but may not be able to connect to the centralized authority 200 (or may not want to connect to the centralized authority 200). As the second device 100 is not directly connected to the centralized authority 200 there may not be a direct communicational channel with the centralized authority 200. This may create trust issues because the second device 100 has to rely on the first device 100 to relay messages 510 between the second device 100 and the centralized authority 200. The centralized authority 200 can use a public key 502 for the second device 100 to secure messages 510 for the second device 100 by making them not readable by the first device 100 without access to the corresponding private key 530 for the second device 100. The secured message 510 can include the response 518 to the access request 506 by the first device 100 so that the first device 100 cannot tamper with or otherwise read the response 518.

[0072] In some embodiments, the first device 100 may not be simultaneously connected to the second device 100 and the centralized authority 200. In some embodiments, the first device 100 may not be initially connected to the centralized authority 200. In such a case, the first device 100 can store the access request 506 in a data cache. Upon detection of a connection to the centralized authority 200, the first device 100 is operable to retrieve the requests 506 in the data cache for transmission to the centralized authority 200. In some embodiments, the first device 100 may not be initially connected to the second device 100. The first device 100 may have an identifier for the second device 100 and an identifier for one or more resources of the second device 100. Prior to connecting to the second device 100, the first device 100 can transmit a request 506 to the centralized authority 200 for access to the one or more resources of the second device 100. The first device 100 receives a response 518 (which may be enclosed in a message 510 or otherwise encrypted) to the request 506. The first device 100 is operable to store the response 518 in a data cache. Upon detection of a connection to the

second device 100, the first device is operable to retrieve the stored response 518 and transmit the response 518 to the second device 100 in order to access the one or more resources of the second device 100. That is, once the first device 100 encounters and connects to a second device 100 it may already have the correct response 518 in its data cache to access the resources of the second device 100. This may be helpful if the first device 100 no longer has access to the centralized authority 200 upon connection to the second device 100. If the first device 100 is off-line it can use stored responses 518 in its data cache to access resources of the second device 100. The first device 100 can connect to the centralized authority 200 to transmit a request 506 and receive a response 518 before the first device 100 goes off-line and no longer has access to the centralized authority 200. For example, a use case may be an airplane flight when prior to the flight the first device 100 can connect to the centralized authority 200 to transmit a request 506 and receive a response 518. During the flight the first device 100 may not be able to connect to the centralized authority 200 but can still connect to the second device 100 to access its resources using the response 518 saved in its data cache. Accordingly, the first device 100 needs to connect with the centralized authority 200 in order to get a response 518 to its request 506 but does not necessarily need a connection to the centralized authority 200 at the time it gains access to the resources of the second device 100 using the response 518. In some example embodiments, responses 518 may be associated with a valid time period. The first device 100 can only use a response 518 to access one or more resources of the second device 100 within the valid time period.

[0073] In some embodiments, the first device 100 can connect to multiple devices 100 and transmit multiple requests 506 to the centralized authority 200 to access different resources from the multiple devices 100. A request 506 can identify one or more devices 100 and one or more corresponding resources for the devices 100. As noted, the first device 100 may not be simultaneously connected to multiple devices 100 and the centralized authority 200 but may still transmit requests 506 to obtain responses 518 for future access to the resources of the second devices 100. Accordingly, the first device 100 may store in its data cache a plurality of responses 518 for access to resources at a plurality of second devices 100.

[0074] In some embodiments, both the first device 100 and the second device 100 can be connected to the centralized authority 200. The centralized authority 200 is operable to directly transmit a response 518 to the second device 100. In some embodiments, the second device can be unpowered and the first device is operable to provide a power source to the second device to retrieve an identifier of the second device 100 or for the second device 100 to process

the response 518 to provide access to its resources. In some embodiments, the Nanoport connector 12 can trigger the first device 100 to provide power to the second device 100. The second device 100 can be a peripheral device that does not have to be attached to a power source, for example.

[0075] The first device 100 is configured to request access to resources of the second device 100 (or other devices 100) using the centralized authority 200. The first device 100 has one or more connectors 12 to establish a connection link to the second device 100 having one or more resources. The first device 100 has a processor configured to transmit an access request 506 to the centralized authority 200. The access request 506 requests access to the one or more resources of the second device 100 using the connection link. The first device 100 is configured to receive a response 518 to the access request 506 from the centralized authority 200. For example, the first device is configured to receive a message 510 that includes the response 518 for the first device 100 to relay to the second device 100. The response 518 includes instructions to instruct the second device 100 to allow (or deny) the first device 100 access to the one or more resources using the connection link. The message 510 that includes the response 518 is encoded to be not readable by the first device 100 and readable by the second device 100. For example, the message 510 can include a portion 524 for that is encrypted using a public key 502 of the second device 100 and can be decrypted using a private key 530 of the second device 100. The private key 530 of the second device 100 may not be accessible by the first device 100. The first device 100 is configured to transmit the response 518 (as part of message 510) to the second device 100 using the connection link. The first device 100 is configured to access the one or more resources of the second device 100 using the connection link. In some embodiments, the first device 100 is configured to receive an identifier for the second device 100 from the second device 100 and transmit the second device identifier to the centralized authority 200 with or as part of the access request 506. In some embodiments, the first device 100 includes a power supply and the processor is configured to transfer power from the power supply to the second device 100 to access the one or more resources, transmit the message 510 with the response 518, receive the second device identifier, and so on. The power may be used, for example, by the second device to power receiver electronics to receive and decode the message 510. In some embodiments, the first device 100 has a data storage storing a public key 514 for the centralized authority 200 and a private key 512 for the first device 100, and for caching responses 518 in manners described above.

[0076] The second device 100 is configured to grant access by the first device 100 to its resources based on the response 518. The second device 100 has one or more communication interfaces 540 to establish a connection link to the first device 100 which also has one or more communication interfaces 540 in some embodiments. The second device 100 has one or more resources, including a data storage 542 storing a public key 528 for the centralized authority 200 and a private key 530 for the second device 100. The second device has a processor 544 configured to transmit a device identifier for the one or more resources to the first device 100. The second device 100 is configured to receive an encrypted response 518 to the access request 506 from the first device 100. The access request 506 includes instructions for automatically requesting access to the one or more resources of the second device 100 by the first device 100 using the connection link. The response 518 is generated by the centralized authority 200. The second device 100 is configured to decrypt the response 518 using the public key 528 for the centralized authority 200 and the private key 530 for the second device 100. The response 518 includes instructions to instruct the second device 100 to allow the first device 100 to access its resources. The second device 100 is configured to allow access by the first device 100 to its one or more resources using the connection link.

[0077] The centralized authority 200 is configured to provision access to resources. The centralized authority 200 includes a persistent data repository storing access right records 400. The access right records 400 include a first access right record defining a first access right of a first device 100 to one or more resources of a second device 100. The access right may be, for example, an access right to establish a connection link to the second device 100, an access right to write data to a memory resource of the second device 100, an access right to read data from a memory resource of the second device 100, an access right to transfer data to and from a memory resource of the second device 100, an access right to transfer and process data using a processing resource of the second device 100, an access right to display data using a display device resource of the second device 100, an access right to receive data from an input device resource of the second device 100, an access right to capture data using a sensor resource of the second device 100, an access right to activate an actuator resource of the second device 100, and so on.

[0078] The centralized authority 200 receives an access request 506 from the first device 100. The access request 506 requests access by the first device 100 to the one or more resources of the second device 100 using a connection link between the first device 100 and the second device 100. The centralized authority 200 is configured to process the access request

506 by verifying the access request 506 against the access right records 400 to determine whether to permit or deny access to some or all of the requested resources.

[0079] The centralized authority 200 is configured to generate a response 518 to the access request 506. The response 518 can permit or deny access to some or all of the resources of the second device 100. The centralized authority 200 generates a message 510 for the first device 100 to relay to the second device 100. The message 510 can include or embed the response 518. If the response 518 permits access then the response 518 includes instructions to instruct the second device 100 to allow the first device 100 to access the one or more resources using the connection link. The message 510 (that includes the response 518) is encoded by the centralized authority 200 to be not readable by the first device and readable by the second device 100. In some embodiments, the centralized authority 200 is configured to transmit the response 518 (enclosed in message 510) to the first device 100 to be relayed to the second device 100. This may be helpful if the second device 100 is not connected to the centralized authority 200. For example, the second device 100 may not have the capacity to connect to the centralized authority or might not otherwise want to connect due to roaming charges, power conservation, and so on. In some embodiments, the centralized authority 200 is configured to transmit the response 518 directly to the second device 100.

[0080] The centralized authority 200 has persistent data repository (e.g., database 300) storing a server private key 504. The centralized authority 200 is configured to encrypt or encode the response 518 using the server private key 504 for decryption by the second device using a corresponding server public key 528. The persistent data repository also stores public keys 502 for different devices 100. The centralized authority 200 is configured to encrypt or encode the response 518 (or a message 510 embedding the response 518) using a public key 502 linked to the second device 100 for decryption by the second device 100 using a corresponding private key 530. The centralized authority 200 is also configured to encrypt or encode a message 508 for the first device using a public key 502 linked to the first device 100 for decryption by the first device 100 using a corresponding private key 512. The centralized authority 200 is configured to include a symmetric key within each of the messages 508, 510. As noted the centralized authority 200 may be in communication with the first device 100 but not in communication with the second device 100. Accordingly, centralized authority 200 may transmit the message 508 to the first device 100 for use by first device 100 and transmit the message 510 (and the response 518) to the first device 100 for relay to the second device 100.

The message 510 (and the response 518) is not readable by the first device 100 as it does not have access to the private key of the second device 100.

[0081] The centralized authority 200 is configured to receive access requests 506 from multiple devices 100. Although in the above examples, first device 100 requests access to resources at second device 100, second device 100 can also request access to resources at first device 100 in some embodiments. There can be an exchange of resources between the devices 100, under the access control of authority 200. The centralized authority 200 is configured to receive multiple access requests from the first device 100 in order to access different resources from different devices 100. The centralized authority 200 is configured to receive and process the additional access request 506. For example, the centralized authority 200 is configured to receive an access request 506 from the first device 100 to request access by the first device 100 to one or more resources of third device (not shown). The centralized authority 200 is configured to store access right records associated with the third device. The centralized authority 200 is configured to process the second access request by verifying the second access request against the access right records linked to the third device. The centralized authority 200 is configured to generate an additional response with instructions to instruct the third device to allow the first device 100 to access the one or more resources using the connection link. The additional response can be encoded to be not readable by the first device 100 and readable by the third device. For example, the centralized authority 200 is configured to encrypt or encode the additional response using a public key 502 associated with the third device. The first device 100 can relay the response to the third device using a connection link. The response can deny the access request in some embodiments. The response can permit access by the first device 100 to the resources of the third device in some embodiments.

[0082] Referring to **FIG. 6**, there is shown a workflow diagram of a method 600A for provisioning access to resources using the system 500 of **FIG. 5**. The method 600A includes operations for first device 100 to obtain access to a resource at a second device 100 using a centralized authority 200.

[0083] At 602, the first device 100 or user associated therewith authenticates with the centralized authority 200. For example, the first device 100 may transmit credentials (e.g., username, password, digital token, handle) to the centralized authority 200. The centralized

authority 200 then verifies the credentials to authenticate the first device 100 or the user associated therewith.

[0084] At 604, the first device 100 can receive a unique identifier (UID) from the second device 100. For example, the first device 100 can receive the unique identifier by way of data transfer through Nanoport connectors 12 or Bluetooth, near field communication (NFC), radio frequency identification (RFID), and so on. In some embodiments, the first device 100 can receive a unique identifier (UID) from centralized authority 200. For example, authority 200 may maintain a registry of locations of various devices and send first device 100 a list of UIDs of proximate second devices 100. In some embodiments, the first device 100 can store the unique identifier in a data cache for subsequent access. In some embodiments, the first device 100 may transmit a message to the second device 100 requesting the unique identifier. In some embodiments, the second device 100 can automatically transmit the unique identifier to the first device 100, such as upon detecting that a connection link has been established with the first device 100. In some embodiments, the first device 100 includes a power source that provides power to the second device 100 in order to receive the unique identifier.

[0085] At 606, the first device 100 transmits an access request 506 to the centralized authority 200. The access request 506 is an electronic data structure with instructions requesting access to one or more resources of the second device 100. The first device 100 can access the one or more resources of the second device 100 using a connection link between the first device 100 and the second device 100. The access request 506 can include a unique identifier for the first device 100, a unique identifier for a user associated with the first device 100, the unique identifier for the second device 100, or combination thereof. The access request 506 can also include identifiers for the one of or more resources of the second device as well as a scope of requested access (read privileges, write privileges, and so on). In some embodiments, a unique identifier for the first device 100 and the unique identifier for the second device 100 are transmitted along with the access request 506.

[0086] At 608, the first device 100 receives a response to the access request 506 from the centralized authority 200. As shown in **FIG. 5**, the response can include multiple messages. For example there may be a first message 508 (message A) for the first device 100 and a second message 510 (message B) for the second device 100. The message 508 for the first device can be encoded or encrypted so that it is only readable by the first device 100. For example, the message 508 for the first device 100 can include a portion 520 encrypted using a public key 502

for the first device 100 and a portion 522 encrypted using a private key 504 for the centralized authority 200. The portion 522 encrypted using a private key 504 for the centralized authority 200 can be embedded within the portion 520 encrypted using a public key 502 for the first device 100. In some embodiments, the order can also be reversed so that portion 520 is embedded in portion 522.

[0087] The message 510 for the second device may be encoded or encrypted so that is not readable the first device 100. For example, the message 510 for the second device 100 can include a portion 524 encrypted using a public key 502 for the second device 100 and a portion 526 encrypted using a private key 504 the centralized authority 200. The portion 526 encrypted using a private key 504 of the centralized authority 200 can be embedded within the portion 524 encrypted using a public key 502 for the second device 100 in some embodiments. In some embodiments, the order can also be reversed so that the portion 524 encrypted using a public key 502 for the second device 100 is embedded in the portion 526 encrypted using a private key 504 of the centralized authority 200.

[0088] At 610, the first device 100 decodes or decrypts at least a portion of the response using a private key of the first device and a public key of the centralized server. For example, the first device 100 can decrypt a portion 520 of the message 508 using a private key 512 for the first device 100. The first device 100 can decrypt a portion 522 of the message 508 using a public key 514 for the centralized authority 200. This may verify that the message 508 was generated and transmitted from the centralized authority 200 using the private key 504 of the centralized authority 200.

[0089] At 612, the first device 100 transmits at least a portion of the response to the second device 100 using the connection link. For example, the first device 100 can transmit a message 510 readable by the second device 100 that was received by the first device 100 as part of the response. As noted above, the portion of the response for the second device may be encoded or encrypted so that is not readable by the first device 100. The second device 100 decodes or decrypts the portion of the response prior to granting access to the one or more resources. For example, the second device 100 can decrypt a portion 524 of the message 510 using a private key 530 of the second device 100. The second device 100 can decrypt a portion 526 of the message 510 using a public key 528 of the centralized authority 200 to obtain the response to the request (and the instruction to approve or deny the access to resources). This may verify that the message 510 was generated and transmitted from the centralized authority 200 using

the private key 504 of the centralized authority 200. That is, this verifies that the centralized authority 200 was the sender of the message 510 given that the centralized authority 200 has access to its private key 504. In some embodiments, the first device 100 is operable to detect a connection to a second device 100. Upon detection of the connection, the first device 100 is operable to transmit the request 506 to the centralized authority 200 or transmit the response 518 (enclosed in message 510) to the second device 100. Upon detection of the connection, the first device 100 is operable to detect an identifier or name for the second device 100.

[0090] At 614, the second device 100 grants access to the first device 100 to none, some, or all of the requested resources, as instructed in response 518. The first device 100 accesses the one or more resources of the second device 100 for which access has been granted using the connection link.

[0091] Referring to **FIG. 7**, there is shown another flowchart diagram of an example method 600B for provisioning access to resources using the system 500 of **FIG. 5** according to some embodiments. As noted, in some embodiments, the system 500 uses a symmetric key to establish a secure communication channel between the first device 100 and the second device 100. Similar to the method 600A of **FIG. 6**, the method 600B includes operations for first device 100 to obtain access to a resource at a second device 100 using a centralized authority 200 as illustrated by the corresponding reference numerals.

[0092] The first device 100 and the second device 100 can receive the symmetric key from the centralized authority 200 as part of the response or otherwise with the response. The centralized authority 200 is configured to generate or retrieve a symmetric key for the first device 100 and the second device 100. As noted, the response can include a message 508 readable by the first device 100 and a message 510 readable by the second device 100. The message 508 readable by the first device 100 can include the symmetric key 516. For example, a portion 522 of the message 508 can include the symmetric key 516. The portion 522 can be encrypted using a private key 504 of the centralized authority 200 to verify that the symmetric key 516 was sent from the centralized authority 200 and not spoofed by a third party, for example. The portion 522 of the message 508 can be embedded within a portion 520 of the message 508 encrypted using the public key 502 of the first device to securely transmit the symmetric key 516 to the first device 100. A portion 526 of the message 510 readable by the second device 100 can also include the symmetric key 516. The message 510 readable by the second device 100 can include the symmetric key 516. The message 510 can be encrypted

using a private key 504 of the centralized authority 200 to verify that the symmetric key 516 was sent from the centralized authority 200 and not spoofed by third party, for example. The portion 526 of the message 510 can be embedded within a portion 524 of the message 510 encrypted using the public key 502 of the second device 100 to securely transmit the symmetric key 516 to the second device 100.

[0093] At 616, the first device 100 and the second device 100 use the symmetric key to establish a secure communication link by encrypting and decrypting messages and data exchanged between the first device 100 and the second device 100. The first device 100 can use a symmetric key to encrypt messages and data transmitted to the second device 100. The second device 100 can use the symmetric key to decrypt the messages and data received from the first device 100. The second device 100 can use the symmetric key to encrypt messages and data to be transmitted to the first device 100. In the first device 100 can use the symmetric key to decrypt messages and data received from the second device 100. Accordingly, the symmetric key can be used to secure data and messages relating to the use of the one or more resources at the second device 100.

[0094] In some embodiments, prior to transmitting the at least a portion of the response to the second device 100 using the connection link at 612, the first device 100 encrypts the portion of the response using the symmetric key. In some embodiments, the first device 100 transmits the symmetric key to the second device as part of the at least a portion of the response at 612. The second device 100 has access to the symmetric key in order to decrypt the portion of the response received from the first device 100. Accordingly, the operations 612 and 616 may be combined in some embodiments.

[0095] Accordingly, various embodiments described herein relate to process 600A, 600B for provisioning access to resources using a centralized authority 200. A first device 100 transmits an access request 506 to the centralized authority 200. The access request 506 requests access to one or more resources of a second device 100 by the first device 100 using a connection link between the first device 100 and the second device 100. The first device 100 receives a response 518 to the access request 506 from the centralized server. As noted, the response 518 can be embedded within a message 510 encrypted to be readable by the second device 100 and to not be readable by the first device 100. The centralized authority 200 transmits a message 508 readable by the first device 100. The message 508 can be transmitted along with the message 510 that includes the response 518. In some embodiments, the

message 508 can include or embed the message 510. In some embodiments, the message 508 can be encrypted or encoded to only be readable by the first device 100. The first device 100 is configured to decrypt the message 508 using a private key 512 and public key 514 stored at or accessible by the first device 100. The message 508 can be referred to as a portion of the response to the request 506 by the centralized authority 200. The first device 100 is configured to transmit a message 510 to the second device 100 using the connection link. The message 510 can be referred to as a portion of the response to the request 506 by the centralized authority 200. If the response 518 grants access to the resources, then the first device 100 accesses the one or more resources of the second device 100 using the connection link after sending the message 510 to the second device 100.

[0096] In some embodiments, the first device 100 connects to the second device 100 to receive a unique identifier for the second device 100. The first device 100 transmits the unique identifier as part of or along with the request 506. The first device 100 is configured to provide power to the second device 100 in order to receive the unique identifier. The first device 100 is also configured to provide power the second device in order to access the one or more resources or transmit the message 510.

[0097] In some embodiments, the centralized authority 200 generates a symmetric key for the first device 100 and the second device 100 to secure communications between the first device 100 and the second device 100. For example, the first device 100 receives the symmetric key 516 from the centralized authority 200 as part of the message 508. The first device receives the symmetric key 516 from the centralized authority 200 to be relayed to the second device 100. The first device 100 transmits the symmetric key 516 to the second device 100 as part of the message 510. The first device 100 and the second device 100 secure the connection link using the symmetric key. For example the symmetric key can be used to encode or encrypt the connection link or data exchanged between the first device 100 and the second device 100 as part of the access to the resources of the second device 100.

[0098] Referring to **FIG. 8**, there is shown another workflow diagram of an example method 800A for provisioning access to resources using the system 500 of **FIG. 5** according to some embodiments.

[0099] At 802, the centralized authority 200 authenticates the first device 100. As noted, the centralized authority 200 is operable to authenticate the first device 100 by processing and

verifying credentials received from the first device 100. The first device 100 can transmit an authentication request to the centralized authority 200 which includes the credentials. In some embodiments, the access request 506 can include the credentials and can be used by the centralized authority 200 to authenticate the first device 100.

[0100] At 804, the centralized authority 200 receives an access request 506 from the first device 100. The access request 506 includes instructions requesting access by the first device 100 to the one or more resources of the second device 100. If the requested 506 is granted, the first device 100 may access the one or more resources of the second device using a connection link between the first device 100 and the second device 100. In some embodiments, the access request 506 can be encrypted using a private key 512 associated with the first device 100. The centralized authority 200 can decrypt the access request 506 using a public key 502 associate with the first device 100. This provides a mechanism to verify the access request 506 was actually received from the first device 100. As noted, the access request 506 can include credentials or other data used by the centralized authority 200 to authenticate the first device at 802. In some embodiments, the first device 100 can receive a unique identifier for the second device 100 by way of data transfer through the Nanoport connectors 12 or another connection link. The first device 100 can generate an access request 506 that includes the unique identifier for the second device 100, along with that identifier for the first device 100 and an identifier for one or more resources of the second device 100 that the first device 100 wishes to access. Accordingly, the access request 506 can include the unique identifier for the second device 100, one or more identifiers for the one or more resources of the second device 100, a unique identifier for the first device 100, and other data used to authorize the first device 100 and otherwise identify the requested resources.

[0101] At 806, the centralized authority 200 processes the access request 506 by verifying the access request 506 against the access right records (stored in a data structure 400 for example) stored in database 300. Centralized authority 200 processes the access request 506 and determines whether or not to grant access to some or all of the requested resources. For example, centralized authority 200 processes the access request with reference to access right records stored in database 300. The access right records can define the scope (e.g., such scope may circumscribe access by time of day, duration, geographic location) of permitted access by one or more devices to one or more resources of other devices. The access right records can include different user profiles that in turn include access rights for various devices associate with the user or the user wishes to access. Accordingly, the centralized authority 200

processes the access request 506 by determining whether or not to grant access to some or all of the requested resources (e.g., with reference to access rights stored in database 300).

[0102] At 808, the centralized authority 200 generates a response to the access request 506. Centralized authority 200 creates a response to the access request 506 based on the results of the processing. The response includes a message 510 for the first device 100 to relay to the second device 100. If the processing indicates that the first device 100 is approved for access to some or all of the resources, then the message 510 includes instructions to instruct the second device 100 to allow the first device 100 to access the one or more resources using the connection link. The instructions can be program code to automatically instruct the second device 100 to allow the first device 100 to access the one or more resources. If the processing indicates that the first device 100 is denied for access for some or all of the resources, then the message 510 includes instructions to instruct the second device 100 to deny the first device 100 to access the one or more resources using the connection link. The response may be valid for particular time range based on when the access request was received or verified. For example, the response may be valid for one day so that the first device 100 can access the resources of the second device 100 for the one day time from based on that response. If the first device 100 wants to access the resources on another day then the first device 100 may need to send an additional access request 506 to the centralized authority 200.

[0103] At 810, the centralized authority 200 encodes or encrypts the message 510 to be not readable by the first device 100 and readable by the second device 100. As shown in **FIG. 5**, the centralized authority 200 maintains a registry of public keys 502 for different devices 100. The registry can be stored in database 300. The public keys 502 can be linked to different devices 100 using unique identifiers for the devices 100. The centralized authority 200 is configured to identify the public key 502 for the second device 100 using the unique identifier for the second device 100 as received from the first device 100 as part of the access request 506 or otherwise directly or indirectly associated with the access request 506. For example the access request 506 may uniquely identify a resource of the second device 100 in the centralized authority 200 is configured to associate the resource with the unique identifier of the second device 100 using a table or other data structure linking resources to devices 100. At least part of the message 510 that contains the response to the access request 506 is encrypted or encoded by the centralized authority 200 using the public key 502 of the second device 100. The part of the message 510 that is encrypted can be decrypted using the private key 530 of the second device 100. The first device 100 does not have access to the private key 530 of the second

device 100 so that the message 510 or portions 524, 526 thereof are not readable by the first device 100. In some embodiments, the centralized authority 200 is configured to generate a hash or digest of the response to the access request 506. The centralized authority 200 is configured to encrypt or encode the hash or digest of the response to be included in the message 510.

[0104] In some embodiments, the centralized authority 200 encodes or encrypts a portion 520 of the message 508 using a public key 502 for the first device 100. The centralized authority 200 encodes or encrypts a portion 522 of the message 508 using a private key 504 for the centralized authority 200. The first device 100 can store or access a public key 514 for the centralized authority 200 and a private key 512 for the first device 100. The public key 514 for the centralized authority 200 and the private key 512 for the first device 100 can be used by the first device to decrypt the portions 520, 522 of the message 508. The centralized authority 200 encodes or encrypts a portion 524 of the message 510 using a public key 502 of the second device 100. The centralized authority 200 encodes or encrypts a portion 526 of the message 510 using a private key 504 of the centralized authority 200. The second device 100 can store or access a public key 528 for the centralized authority 200 and a private key 530 for the second device 100. The public key 528 for the centralized authority 200 and the private key 530 for the second device 100 can be used by the second device 100 to decrypt the portions 524, 526 of the message 510.

[0105] At 812, the centralized authority 200 transmits response 518. As noted, the response 518 may be embedded in a message 510 for the second device 100. The centralized authority 200 is operable to transmit a message 508 for the first device 100 along with the response 518.

[0106] Referring to **FIG. 9**, there is shown another example method 800B for provisioning access to resources using the system 500 of **FIG. 5** according to some embodiments. As noted, in some embodiments, a symmetric key 516 can be used to establish a secured communication channel or link between the first device 100 and the second device 100. Similar to the method 800A of **FIG. 8**, the method 800B includes operations for the centralized authority 200 to approve access by a first device 100 to a resource at a second device 100 as illustrated by the corresponding reference numerals.

[0107] The centralized authority 200 may provide a symmetric key 516 to both the first device 100 and the second device 100 to establish a secured communication channel for use in

association with the requested resource, e.g., to transfer data from a memory resource at second device 100 to first device 100 in a secure way. This is an example and the centralized authority 200 may otherwise make a symmetric key 516 accessible to the first device and the second device in some embodiments.

[0108] At 807, the centralized authority 200 generates or retrieves a symmetric key 516 for the first device 100 and the second device 100 to establish a secured communication channel. For example, the centralized authority 200 can generate or retrieve a symmetric key 516 using the identifier for the first device 100 or the second device. As noted, the secured communication channel can be used to exchange data and messages relating to the access of the resources of the second device 100.

[0109] At 808, the centralized authority 200 creates a message containing the symmetric key 516. As shown, the centralized authority 200 can generate a message 508 readable by the first device 100 and a message 510 readable by the second device 100. The message 508 for the first device 100 can include a symmetric key 516 and the message 510 for the second device can also include the symmetric key 516. As noted, the symmetric key 516 can be used by the first device and the second device 100 to create a secure communication link between the first device 100 and the second device 100. The message 510 for the second device can include a response 518 to the access request 506 along with the symmetric key 516. Part of or the entire the message 510 is encrypted using a public key 502 for the second device 100 and a private key 504 for the centralized authority 200. The second device 100 stores or accesses a public key 528 for the centralized authority and a private key 530 for the second device 100 to decrypt the message 510 or parts thereof. The centralized authority 200 is operable to maintain a registry of symmetric keys in some embodiments.

[0110] In some embodiments, the centralized authority 200 encodes or encrypts a portion 520 of the message 508 using a public key 502 for the first device 100. The centralized authority 200 encodes or encrypts a portion 522 of the message 508 using a private key 504 for the centralized authority 200. The portion 522 can include a symmetric key 516. The first device 100 can store or access a public key 514 for the centralized authority 200 and a private key 512 for the first device 100. The public key 514 for the centralized authority 200 and the private key 512 for the first device 100 can be used by the first device to decrypt the portions 520, 522 of the message 508. The centralized authority 200 encodes or encrypts a portion 524 of the message 510 using a public key 502 of the second device 100. The centralized authority 200 encodes or

encrypts a portion 526 of the message 510 using a private key 504 of the centralized authority 200. The portion 526 can include a symmetric key. The second device 100 can store or access a public key 528 for the centralized authority 200 and a private key 530 for the second device 100. The public key 528 for the centralized authority 200 and the private key 530 for the second device 100 can be used by the second device 100 to decrypt the portions 524, 526 of the message 510.

[0111] At 812, the centralized authority 200 transmits the response 518. As noted, the response 518 may be embedded in a message 510 readable by the second device 100 and not readable by the first device 100. The centralized authority 200 is operable to transmit a message 508 for the first device 100 along with the response 518. The centralized authority 200 transmits a message 508 to the first device 100. The centralized authority 200 transmits a message 510 to the first device 100 for relay to the second device 100. For example the second device 100 may be unable to connect to the centralized authority 200 to communicate directly with the centralized authority 200 so that the first device 100 is required to relay the message 510 to the second device 100. In some embodiments, the first device 100 provides a power supply to the second device 100 in order for the second device 100 to receive the message 510.

[0112] The first device 100 decrypts the message 508 using its private key 512 to obtain the symmetric key 516. The first device 100 verifies that the message 508 was generated or transmitted by the centralized authority 200 using a public key 514 for the centralized authority 200 as only the centralized authority 200 has access to the corresponding private key 504.

[0113] The first device 100 transmits the message 510 to the second device 100. The second device 100 decrypts the message 510 using its private key 530 to obtain the response 518 to the access request 506 and the symmetric key 516. The second device 100 decrypts the message 510 using a public key 528 for the centralized authority 200 to verify that the centralized authority 200 was the original sender or creator of the message 510 (and the response 518 therein). The second device 100 processes the response 518 to grant access to the first device 100 to some or all of the requested resources. The response 518 includes machine-readable instructions to grant access to some or all of the requested resources. The first device 100 and the second device 100 to establish a secured communication channel using the symmetric key 516.

[0114] In some embodiments, to implement the encryption/decryption steps, devices 100 and the centralized authority 200 may utilize Transport Layer Security (TLS) or Secure Sockets Layer (SSL) libraries.

[0115] In some embodiments, the second device 100 may lack its own power source, e.g., an integral battery or connection to mains power, and may draw power from the first device 100, e.g., through a Nanoport connector 12. Such power may be used by the second device 100 to, e.g., transmit its unique identifier (UID) to the first device 100, to receive and process message 510 or parts thereof.

[0116] In some embodiments, the steps described above to obtain access to a response at the second device 100 may be triggered or preceded by detection at the first device 100 of a Nanoport connection to the second device 100, e.g., as described in U.S. Patent Application No. 62/327826, entitled “MAGNET POSITION DETECTION IN A MAGNETIC CONNECTOR”, the contents of which is hereby incorporated by reference.

[0117] The embodiments of the devices, systems and methods described herein may be implemented in a combination of both hardware and software. These embodiments may be implemented on programmable computers, each computer including at least one processor, a data storage system (including volatile memory or non-volatile memory or other data storage elements or a combination thereof), and at least one communication interface.

[0118] Program code is applied to input data to perform the functions described herein and to generate output information. The output information is applied to one or more output devices. In some embodiments, the communication interface may be a network communication interface. In embodiments in which elements may be combined, the communication interface may be a software communication interface, such as those for inter-process communication. In still other embodiments, there may be a combination of communication interfaces implemented as hardware, software, and combination thereof.

[0119] Throughout the foregoing discussion, numerous references will be made regarding servers, services, interfaces, portals, platforms, or other systems formed from computing devices. It should be appreciated that the use of such terms is deemed to represent one or more computing devices having at least one processor configured to execute software instructions stored on a computer readable tangible, non-transitory medium. For example, a

server can include one or more computers operating as a web server, database server, or other type of computer server in a manner to fulfill described roles, responsibilities, or functions.

[0120] Various example embodiments are described herein. Although each embodiment represents a single combination of inventive elements, all possible combinations of the disclosed elements include the inventive subject matter. Thus if one embodiment comprises elements A, B, and C, and a second embodiment comprises elements B and D, then the inventive subject matter is also considered to include other remaining combinations of A, B, C, or D, even if not explicitly disclosed.

[0121] The term “connected” or "coupled to" may include both direct coupling (in which two elements that are coupled to each other contact each other) and indirect coupling (in which at least one additional element is located between the two elements).

[0122] The technical solution of embodiments may be in the form of a software product. The software product may be stored in a non-volatile or non-transitory storage medium, which can be a compact disk read-only memory (CD-ROM), a USB flash disk, or a removable hard disk. The software product includes a number of instructions that enable a computer device (personal computer, server, or network device) to execute the methods provided by the embodiments.

[0123] The embodiments described herein are implemented by physical computer hardware, including computing devices, servers, receivers, transmitters, processors, memory, displays, and networks. The embodiments described herein provide useful physical machines and particularly configured computer hardware arrangements. The embodiments described herein are directed to electronic machines and methods implemented by electronic machines adapted for processing and transforming electromagnetic signals which represent various types of information.

[0124] For simplicity only one centralized authority 200 is shown but system may include multiple centralized authorities 200 to provision access to resources of devices 100. The first device 100 and the second device 100 may be the same or different types of devices. The first device 100 can it include at least one processor, a data storage device (including volatile memory or non-volatile memory or other data storage elements or a combination thereof), and at least one communication interface. The device 100 components may be connected in various ways including directly coupled, indirectly coupled via a network, and distributed over a wide geographic area and connected via a network (which may be referred to as “cloud computing”).

The communication interface can include at least one I/O interface, and at least one network interface. The centralized authority 200 can it include at least one processor, a data storage device (including volatile memory or non-volatile memory or other data storage elements or a combination thereof), and at least one communication interface. The centralized authority 200 components may be connected in various ways including directly coupled, indirectly coupled via a network, and distributed over a wide geographic area and connected via a network (which may be referred to as “cloud computing”). The communication interface can include at least one I/O interface, and at least one network interface.

[0125] The processor may be, for example, any type of general-purpose microprocessor or microcontroller, a digital signal processing (DSP) processor, an integrated circuit, a field programmable gate array (FPGA), a reconfigurable processor, or any combination thereof.

[0126] Memory may include a suitable combination of any type of computer memory that is located either internally or externally such as, for example, random-access memory (RAM), read-only memory (ROM), compact disc read-only memory (CDROM), electro-optical memory, magneto-optical memory, erasable programmable read-only memory (EPROM), and electrically-erasable programmable read-only memory (EEPROM), Ferroelectric RAM (FRAM) or the like.

[0127] The I/O interface enables the device 100 to interconnect with one or more I/O devices, such as a keyboard, mouse, camera, touch screen and a microphone, or with one or more output devices such as a display screen and a speaker.

[0128] The network interface enables the device 100 or centralized authority 200 to communicate with other components, to exchange data with other components, to access and connect to network resources, to serve applications, and perform other computing applications by connecting to a network (or multiple networks) capable of carrying data.

[0129] The first device is operable to register and authenticate users (using a login, unique identifier, and password for example) prior to implementing the operations described herein. The registration data can be used as credentials for the centralized authority 200 for example. The first device 100 may serve one user or multiple users.

[0130] Although the embodiments have been described in detail, it should be understood that various changes, substitutions and alterations can be made herein without departing from the scope as defined by the appended claims.

[0131] Moreover, the scope of the present application is not intended to be limited to the particular embodiments of the process, machine, manufacture, composition of matter, means, methods and steps described in the specification. As one of ordinary skill in the art will readily appreciate from the disclosure of the present invention, processes, machines, manufacture, compositions of matter, means, methods, or steps, presently existing or later to be developed, that perform substantially the same function or achieve substantially the same result as the corresponding embodiments described herein may be utilized. Accordingly, the appended claims are intended to include within their scope such processes, machines, manufacture, compositions of matter, means, methods, or steps.

[0132] As can be understood, the features described above and illustrated are intended to be examples only.

WHAT IS CLAIMED IS:

1. A centralized server for provisioning access to resources comprising:

a persistent data repository storing access right records including a first access right record with a first access right of a first device to one or more resources of a second device;

a processor configured to:

receive a first access request from the first device, the first access request requesting access by the first device to the one or more resources of the second device using a connection link between the first device and the second device;

process the first access request by verifying the first access request against the access right records;

generate a first response to the first access request, the first response comprising a message for the first device to relay to the second device, the message comprising instructions to instruct the second device to allow the first device to access the one or more resources using the connection link, the first message encoded to be not readable by the first device and readable by the second device; and

transmit the first response.

2. The server of claim 1, wherein the processor is configured to transmit the first response to the second device by transmitting the message to the first device for relay to the second device.

3. The server of claim 1 or claim 2, the persistent data repository storing a public key for the second device, the processor being configured to generate the first response by encrypting at least a portion of the response comprising the message using the public key for the second device, the at least a portion of the first response for decryption by the second device using a corresponding private key for the second device.

4. The server of claim 3, the persistent data repository storing a server private key, the processor being configured to generate the response by encrypting at least the portion of the response using the server private key for decryption by the second device using a corresponding server public key.

5. The server of any one of claims 1 to 4, the message comprising a device identifier for the first device.

6. The server of any one of claims 1 to 5, wherein the message is a first message and the first response further comprises a second message for the first device.

7. The server of claim 6, the persistent data repository storing a public key for the first device, the processor being configured to generate the first response by encrypting at least a portion of the response comprising the second message using the public key for the first device, the at least a portion of the first response for decryption by the first device using a corresponding private key.

8. The server of claim 7, the processor being configured to generate a symmetric key, wherein the first message comprises the symmetric key for the first and second devices to establish a secured communication link.

9. The server of claim 8, wherein the second message comprises the symmetric key.

10. The sever of any one of claims 1 to 9, the persistent data repository linking a first device identifier and the first access right record, the first access request indicating a first device identifier, and the processor being further configured to process the first access request by verifying the first device identifier.

11. The sever of any one of claims 1 to 10, the persistent data repository storing user profiles including a first user profile linking a first user identifier, the second device and the first access right record, the first access request indicating the first user identifier, wherein the processor is configured to process the first access request using the first user profile to locate the first access right record.

12. The server of any one of claims 1 to 11, wherein the first response comprises an access time period having a start time and an end time, wherein the processor is configured to generate the message comprising instructions to instruct the second device to allow the first device to access the one or more resources only during the access time period.

13. The server of any one of claims 1 to 12, the first access right selected from the group consisting of an access right to establish a connection link to the second device, an access right to write data to a memory resource of the second device, an access right to read data from a memory resource of the second device, an access right to transfer data to and from a memory resource of the second device, an access right to transfer and process data using a processing resource of the second device, an access right to display data using a display device resource of the second device, an access right to receive data from an input device resource of the second device, an access right to capture data using a sensor resource of the second device, and an access right to activate an actuator resource of the second device.

14. The server of any one of claims 1 to 13, the first access request identifying the connection link of the one or more connectors between the first device and the second device.

15. The server of any one of claims 1 to 14, the centralized server being in communication with the first device but not in communication with the second device.

16. The server of any one of claims 1 to 15, the persistent data repository storing a first public key in association with the first device, a second public key in association with the second device, and a server private key, the processor being configured to generate the first response by:

generating a symmetric key for the first device and the second device to establish a secure communication channel for inclusion in the first message and the second message;

encrypting at least a portion of the response comprising the message with the second public key and the server private key; and

encrypting at least a portion of the response with the first public key and the server private key.

17. The server of any one of claims 1 to 16 wherein the persistent data repository is configured to store a second access right record with a second access right of the first device to one or more resources of a third device;

the processor further configured to:

receive a second access request from the first device, the second access request requesting access by the first device to the one or more resources of the third device using a second connection link between the first device and the third device;

process the second access request by verifying the second access request against the access right records;

generate a second response to the second access request, the second response comprising a second message for the first device to relay to the third device, the second message comprising instructions to instruct the third device to allow the first device to access the one or more resources using the connection link, the first message encoded to be not readable by the first device and readable by the third device; and

transmit the second response.

18. The server of any one of claims 1 to 17, the processor being configured to:

receive a third access request from the first device, the third access request requesting access by the first device to an additional resource of the second device using the connection link;

process the third access request by verifying the third access request against the access right records;

generate a third response to the third access request, the response denying the third access request; and

transmit the third response.

19. The server of any one of claims 1 to 18, the processor being configured to authenticate the first device by verifying a first user identifier or a first device identifier against the access right records.

20. The server of any one of claims 1 to 19, wherein the first access right record comprises a first device identifier, a second device identifier and a resource identifier, the first access request comprising the first device identifier, the second device identifier and the resource identifier, and the processor being configured to process the first access request by verifying the

access request against the access right records using the first device identifier, the second device identifier and the resource identifier.

21. A process for provisioning access to resources using a centralized server comprising:

transmitting, by a first device, an access request from to the centralized server, the access request requesting access to one or more resources of a second device by the first device using a connection link between the first device and the second device;

receiving a response to the access request from the centralized server, the response comprising a first portion for the first device to relay to the second device and encoded to be not readable by the first device and readable by the second device;

decrypting at least a second portion of the response using a private key of the first device and a public key of the centralized server;

transmitting the first portion of the response to the second device using the connection link; and

accessing, by the first device, the one or more resources of the second device using the connection link.

22. The process of claim 21 further comprising:

receiving a second device identifier; and

transmitting the second device identifier with the access request.

23. The process of claim 21 or claim 22 further comprising providing power from the first device to the second device in order to access the one or more resources or transmit the portion of the response.

24. The process of any one of claims 21 to 23 further comprising:

receiving a symmetric key from the centralized server;

transmitting the symmetric key to the second device as part of the first portion of the response; and

transmitting data encrypted using the symmetric key to the second device.

25. A device for requesting access to resources using a centralized server comprising:

a communication interface to establish a connection link to a second device having one or more resources;

a processor configured to:

transmit an access request to the centralized server, the access request requesting access to the one or more resources of the second device using the connection link;

receive a response to the access request from the centralized server, the first response comprising a portion for the first device to relay to the second device, the portion of the first response comprising instructions to instruct the second device to allow the first device to access the one or more resources using the connection link, the portion of the first response encoded to be not readable by the first device and readable by the second device;

transmit the portion of the first response to the second device using the connection link; and

access the one or more resources of the second device using the connection link.

26. The device of claim 25 wherein the processor is configured to receive a second device identifier and from the second device and transmit the second device identifier with the access request.

27. The device of claim 25 or claim 26 further comprising a power supply wherein the processor is configured to transfer power from the power supply to the second device.

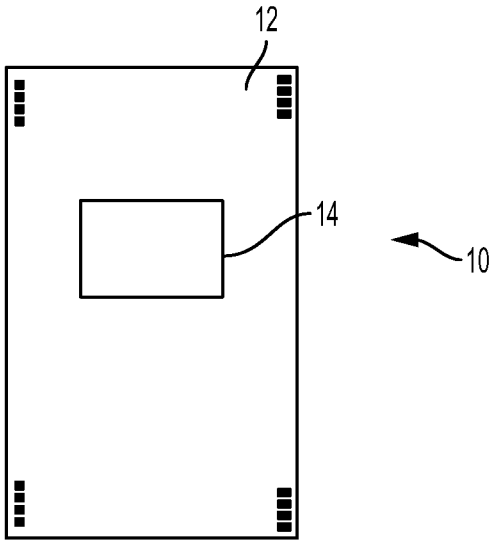

FIG. 1

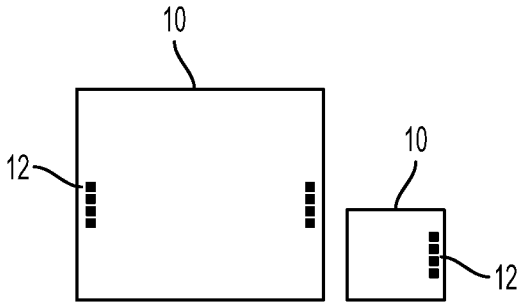

FIG. 2

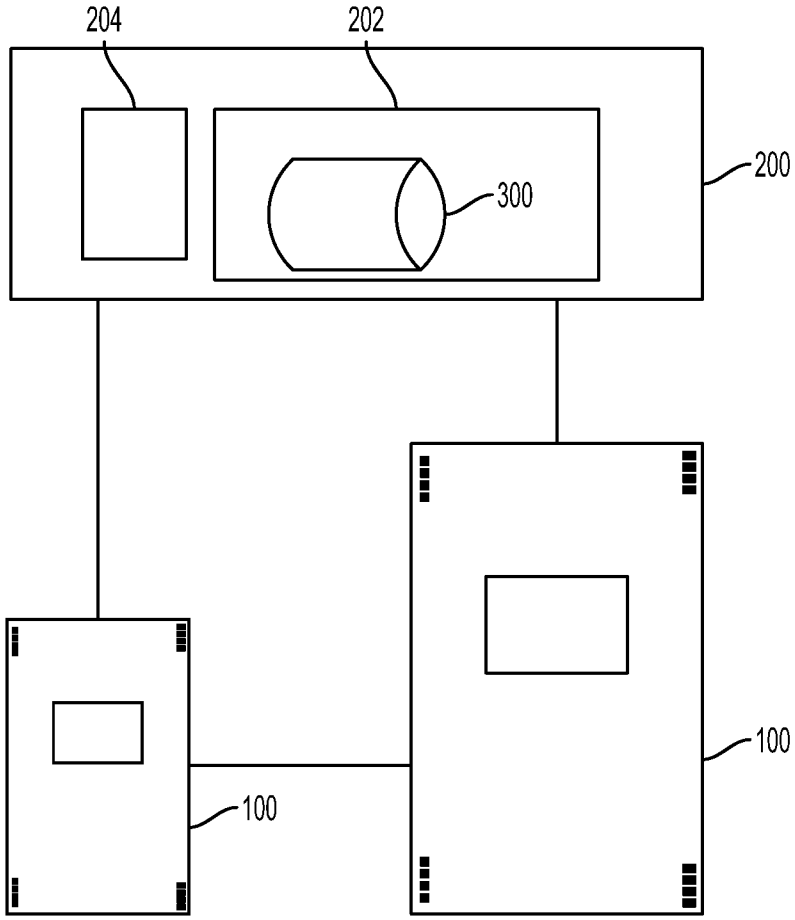

FIG. 3

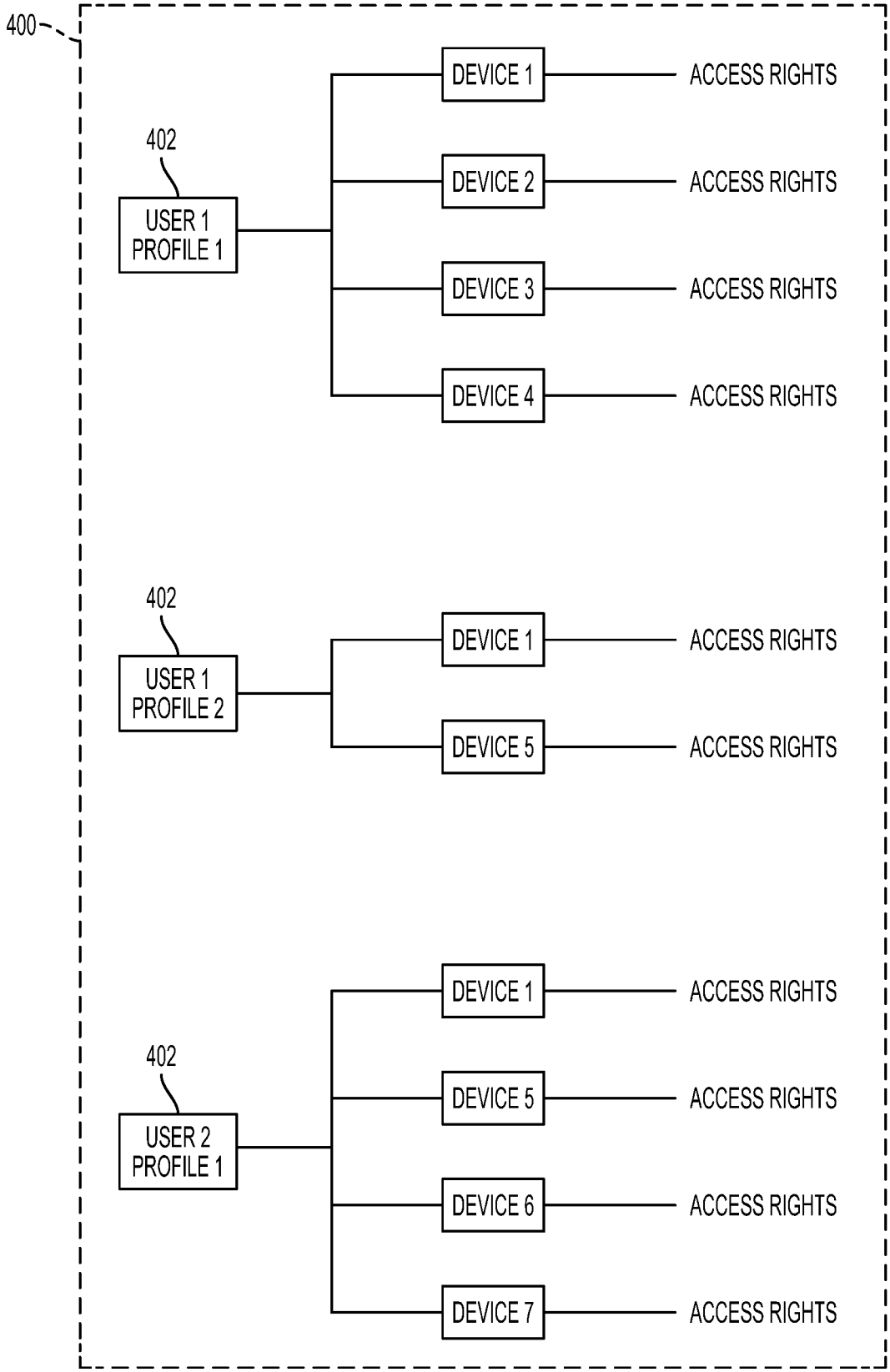
400
402
USER 1 PROFILE 1
DEVICE 1
ACCESS RIGHTS
DEVICE 2
ACCESS RIGHTS
DEVICE 3
ACCESS RIGHTS
DEVICE 4
ACCESS RIGHTS
402
USER 1 PROFILE 2
DEVICE 1
ACCESS RIGHTS
DEVICE 5
ACCESS RIGHTS
402
USER 2 PROFILE 1
DEVICE 1
ACCESS RIGHTS
DEVICE 5
ACCESS RIGHTS
DEVICE 6
ACCESS RIGHTS
DEVICE 7
ACCESS RIGHTS

FIG. 4A

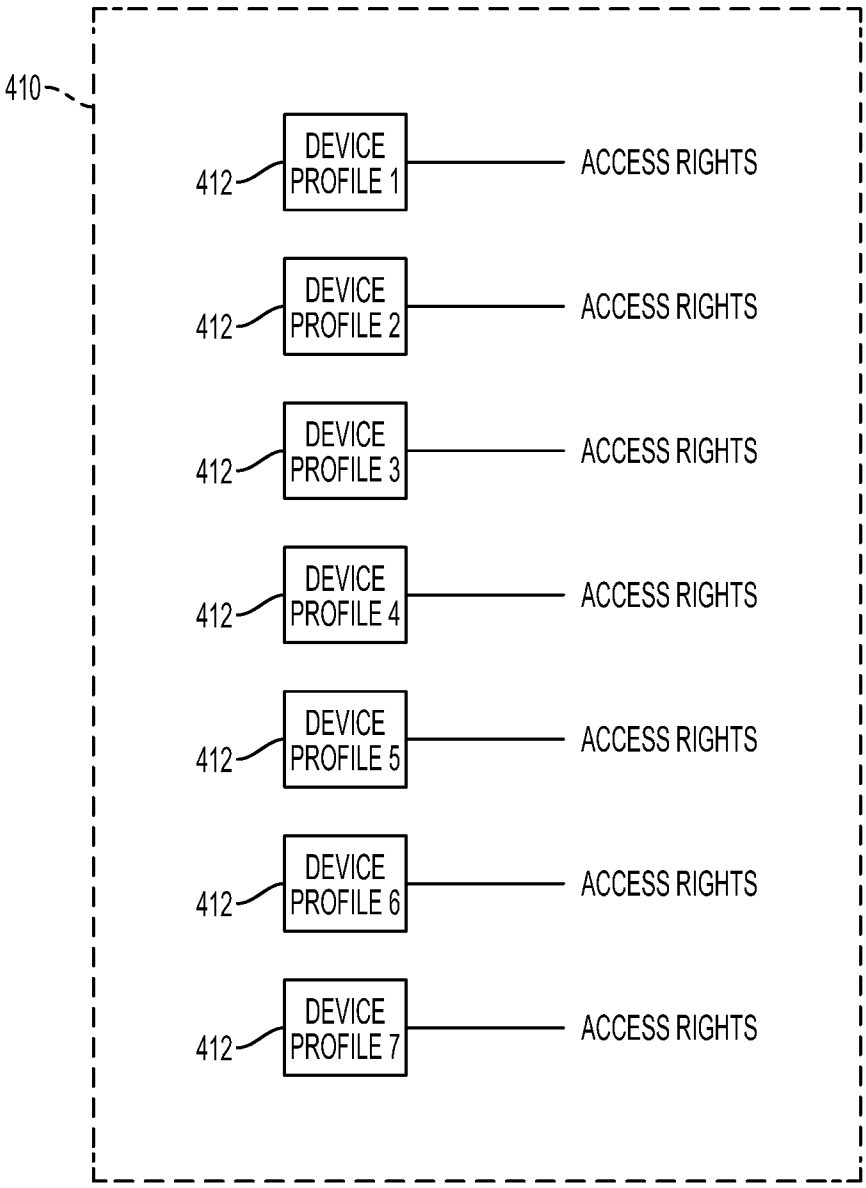
410
412
DEVICE PROFILE 1
ACCESS RIGHTS
412
DEVICE PROFILE 2
ACCESS RIGHTS
412
DEVICE PROFILE 3
ACCESS RIGHTS
412
DEVICE PROFILE 4
ACCESS RIGHTS
412
DEVICE PROFILE 5
ACCESS RIGHTS
412
DEVICE PROFILE 6
ACCESS RIGHTS
412
DEVICE PROFILE 7
ACCESS RIGHTS

FIG. 4B

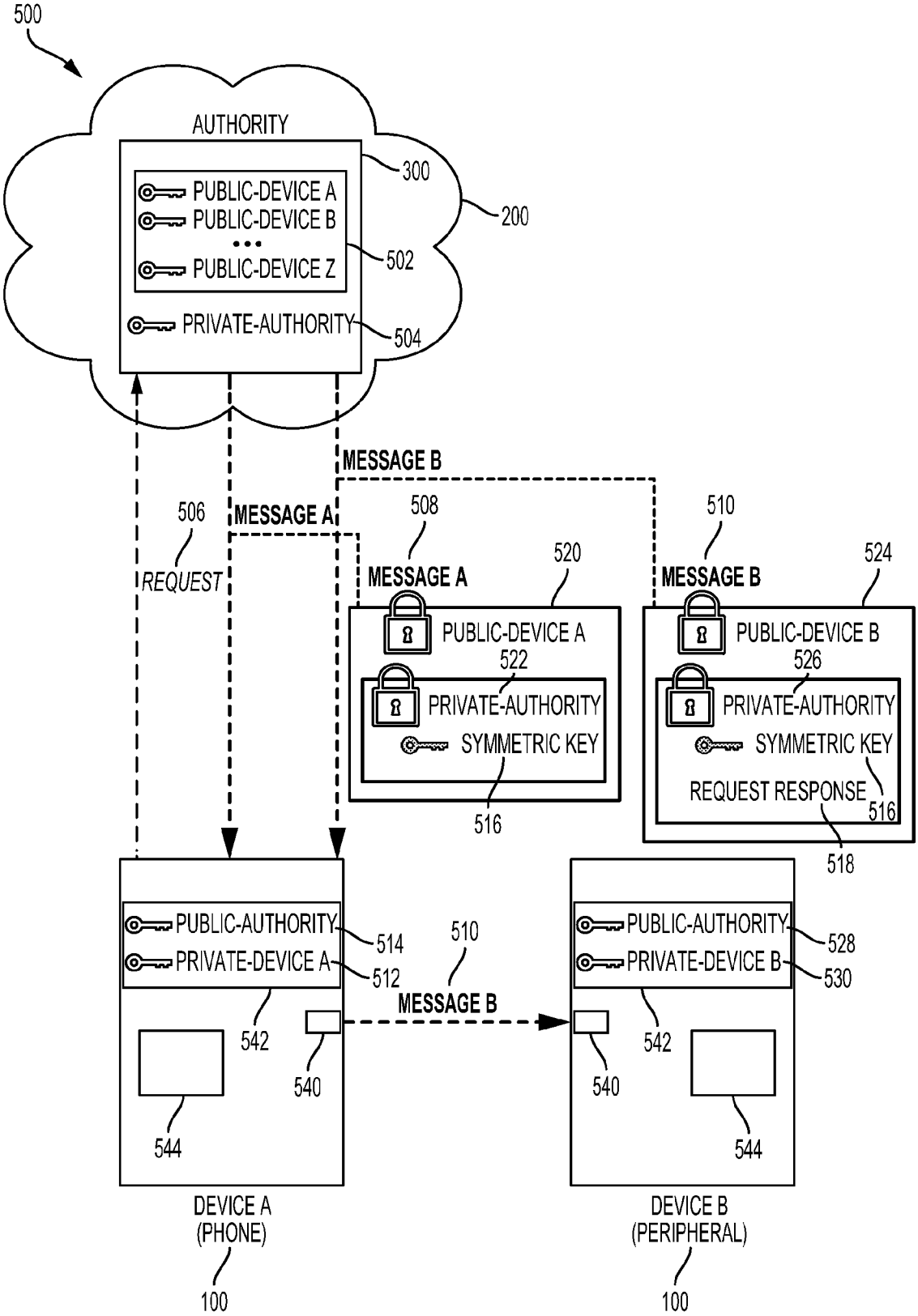
500
AUTHORITY
300
200
PUBLIC-DEVICE A
PUBLIC-DEVICE B
PUBLIC-DEVICE Z
502
PRIVATE-AUTHORITY
504
MESSAGE B
506
MESSAGE A
508
510
REQUEST
MESSAGE A
520
MESSAGE B
524
PUBLIC-DEVICE A
522
PUBLIC-DEVICE B
526
PRIVATE-AUTHORITY
SYMMETRIC KEY
516
PRIVATE-AUTHORITY
SYMMETRIC KEY
REQUEST RESPONSE
516
518
PUBLIC-AUTHORITY
PRIVATE-DEVICE A
514
512
510
MESSAGE B
PUBLIC-AUTHORITY
PRIVATE-DEVICE B
528
530
542
540
542
540
544
544
DEVICE A
(PHONE)
100
DEVICE B
(PERIPHERAL)
100

FIG. 5

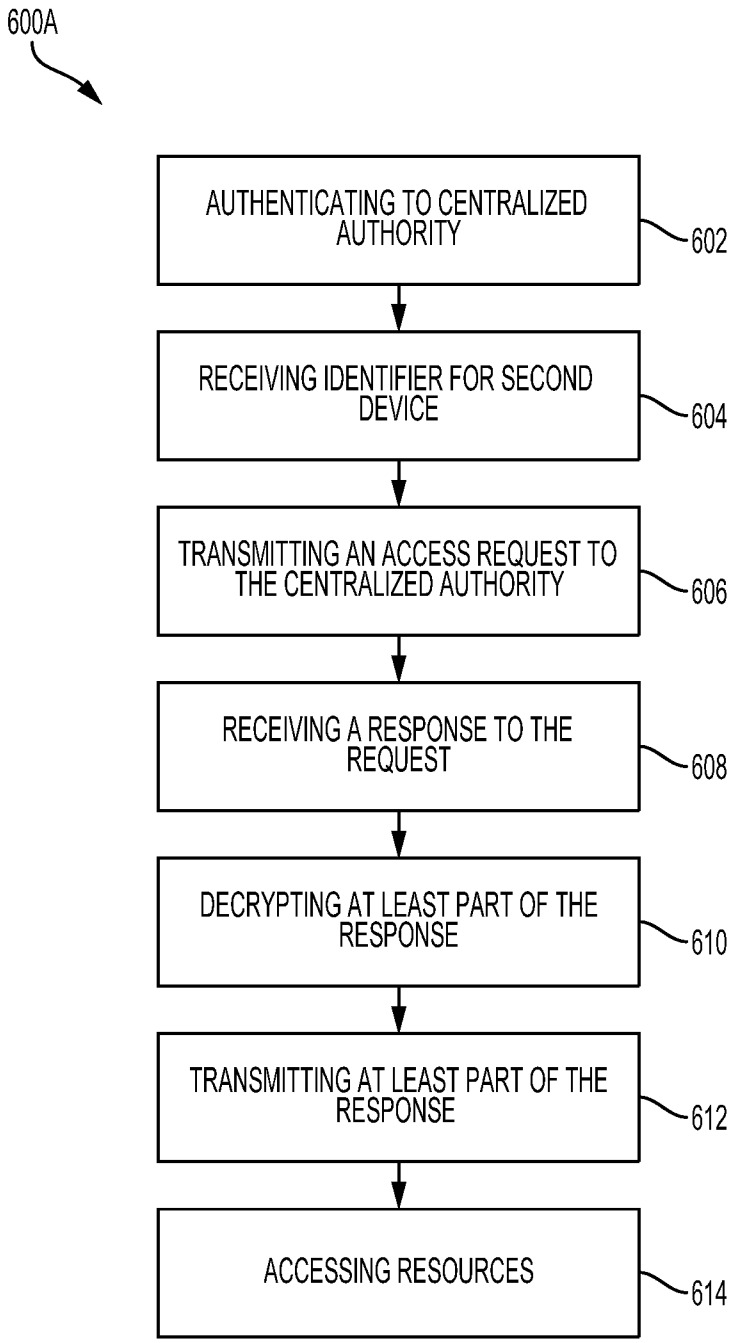
600A
AUTHENTICATING TO CENTRALIZED AUTHORITY
602
RECEIVING IDENTIFIER FOR SECOND DEVICE
604
TRANSMITTING AN ACCESS REQUEST TO THE CENTRALIZED AUTHORITY
606
RECEIVING A RESPONSE TO THE REQUEST
608
DECRYPTING AT LEAST PART OF THE RESPONSE
610
TRANSMITTING AT LEAST PART OF THE RESPONSE
612
ACCESSING RESOURCES
614

FIG. 6

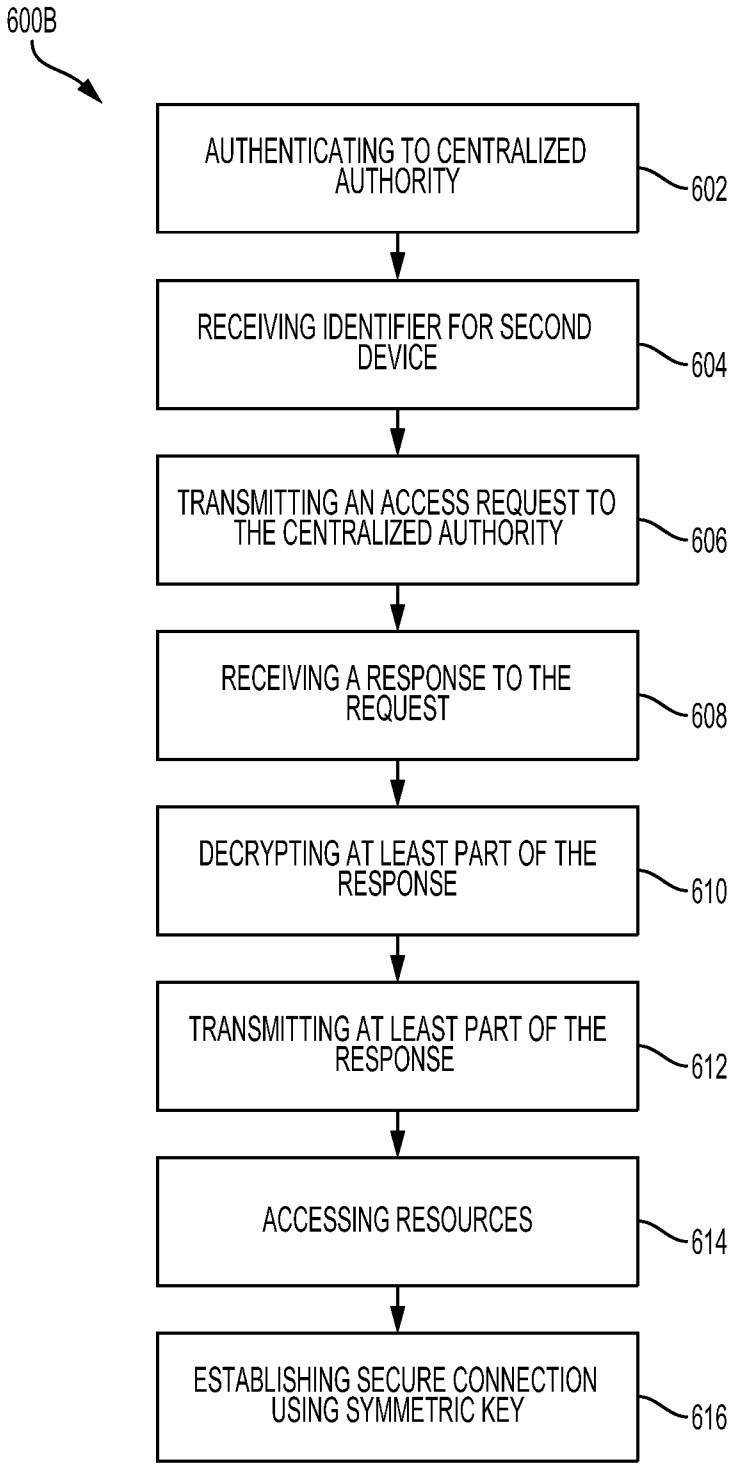
600B
AUTHENTICATING TO CENTRALIZED AUTHORITY
602
RECEIVING IDENTIFIER FOR SECOND DEVICE
604
TRANSMITTING AN ACCESS REQUEST TO THE CENTRALIZED AUTHORITY
606
RECEIVING A RESPONSE TO THE REQUEST
608
DECRYPTING AT LEAST PART OF THE RESPONSE
610
TRANSMITTING AT LEAST PART OF THE RESPONSE
612
ACCESSING RESOURCES
614
ESTABLISHING SECURE CONNECTION USING SYMMETRIC KEY
616

FIG. 7

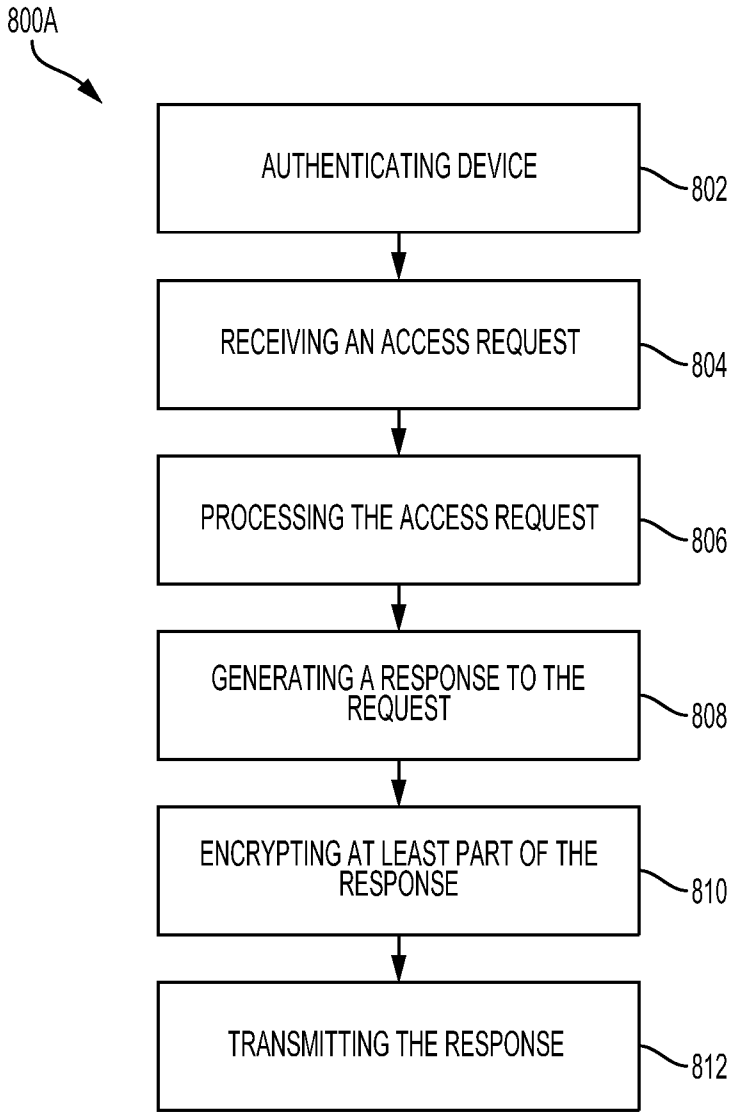
800A
AUTHENTICATING DEVICE
802
RECEIVING AN ACCESS REQUEST
804
PROCESSING THE ACCESS REQUEST
806
GENERATING A RESPONSE TO THE REQUEST
808
ENCRYPTING AT LEAST PART OF THE RESPONSE
810
TRANSMITTING THE RESPONSE
812

FIG. 8

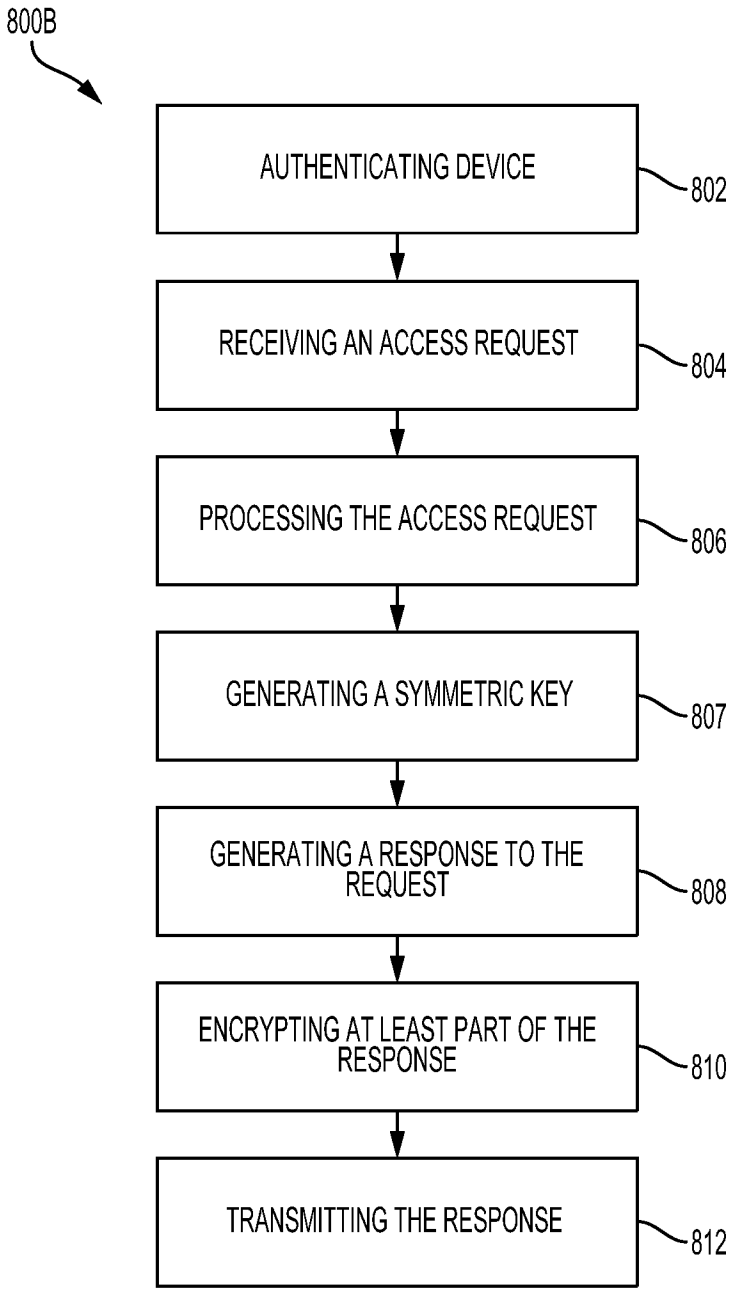
800B
AUTHENTICATING DEVICE
802
RECEIVING AN ACCESS REQUEST
804
PROCESSING THE ACCESS REQUEST
806
GENERATING A SYMMETRIC KEY
807
GENERATING A RESPONSE TO THE REQUEST
808
ENCRYPTING AT LEAST PART OF THE RESPONSE
810
TRANSMITTING THE RESPONSE
812

FIG. 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CA2017/051067

A. CLASSIFICATION OF SUBJECT MATTER
IPC: ***H04L 9/32*** (2006.01) , ***H04L 9/08*** (2006.01) , ***H04L 9/30*** (2006.01)

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)
IPC: ***H04L**** (2006.01), ***H04L 9/32*** (2006.01) , ***H04L 9/08*** (2006.01) , ***H04L 9/30*** (2006.01)

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

Electronic database(s) consulted during the international search (name of database(s) and, where practicable, search terms used)
Databases: Questel-Orbit; Google Patents; Google
Keywords: device-to-device, D2D, access, connection, link, encod*, public key, private key, data repository, server, device interface, provision*, access rights, resource access

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P, A	US 2017/0223005 A1 (BIRGISSON et al.), 3 August 2017 (03-08-2017) *paragraphs [0050-0053], [0057-0072]	1-27
A	WO 2016/109885 A1 (SZETO), 14 July 2016 (14-07-2016) *paragraphs [0026-0028]	1, 21, 25
A	US 2014/0230019 A1 (CIVELLI et al.), 14 August 2014 (14-08-2014) *paragraphs [0024-0033]	1-27
A	US 2009/0300744 A1 (GUO et al.), 3 December 2009 *paragraphs [0020], [0023]	1-27

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

*	Special categories of cited documents:	"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
"A"	document defining the general state of the art which is not considered to be of particular relevance	"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
"E"	earlier application or patent but published on or after the international filing date	"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
"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)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than		

Date of the actual completion of the international search 20 November 2017 (20-11-2017)	Date of mailing of the international search report 18 December 2017 (18-12-2017)
Name and mailing address of the ISA/CA Canadian Intellectual Property Office Place du Portage I, C114 - 1st Floor, Box PCT 50 Victoria Street Gatineau, Quebec K1A 0C9 Facsimile No.: 819-953-2476	Authorized officer Jamie Hayami (819) 639-4735

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CA2017/051067

Patent Document Cited in Search Report	Publication Date	Patent Family Member(s)	Publication Date
US2017223005A1	03 August 2017 (03-08-2017)	US2017223005A1	03 August 2017 (03-08-2017)
		CN107070863A	18 August 2017 (18-08-2017)
		DE102016226311A1	03 August 2017 (03-08-2017)
		DE202016107487U1	04 May 2017 (04-05-2017)
		WO2017131887A1	03 August 2017 (03-08-2017)
WO2016109885A1	14 July 2016 (14-07-2016)	WO2016109885A1	14 July 2016 (14-07-2016)
		US2016210257A1	21 July 2016 (21-07-2016)
US2014230019A1	14 August 2014 (14-08-2014)	US2014230019A1	14 August 2014 (14-08-2014)
		WO2014126987A1	21 August 2014 (21-08-2014)
US2009300744A1	03 December 2009 (03-12-2009)	US2009300744A1	03 December 2009 (03-12-2009)
		US7979899B2	12 July 2011 (12-07-2011)
		CN102047709A	04 May 2011 (04-05-2011)
		CN102047709B	30 October 2013 (30-10-2013)
		EP2283669A2	16 February 2011 (16-02-2011)
		EP2283669A4	24 September 2014 (24-09-2014)
		JP2011522327A	28 July 2011 (28-07-2011)
		JP5038531B2	03 October 2012 (03-10-2012)
		KR20110020783A	03 March 2011 (03-03-2011)
		KR101534890B1	07 July 2015 (07-07-2015)
		US2011247055A1	06 October 2011 (06-10-2011)
		US8800003B2	05 August 2014 (05-08-2014)
		WO2009148746A2	10 December 2009 (10-12-2009)
		WO2009148746A3	22 April 2010 (22-04-2010)