Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2593888 C 2014/09/09

(11)(21) 2 593 888

(12) BREVET CANADIEN
CANADIAN PATENT

(13) C

(22) Date de dépôt/Filing Date: 2007/07/17

(41) Mise à la disp. pub./Open to Public Insp.: 2008/01/20

(45) Date de délivrance/Issue Date: 2014/09/09

(30) Priorité/Priority: 2006/07/20 (EP06117582.4)

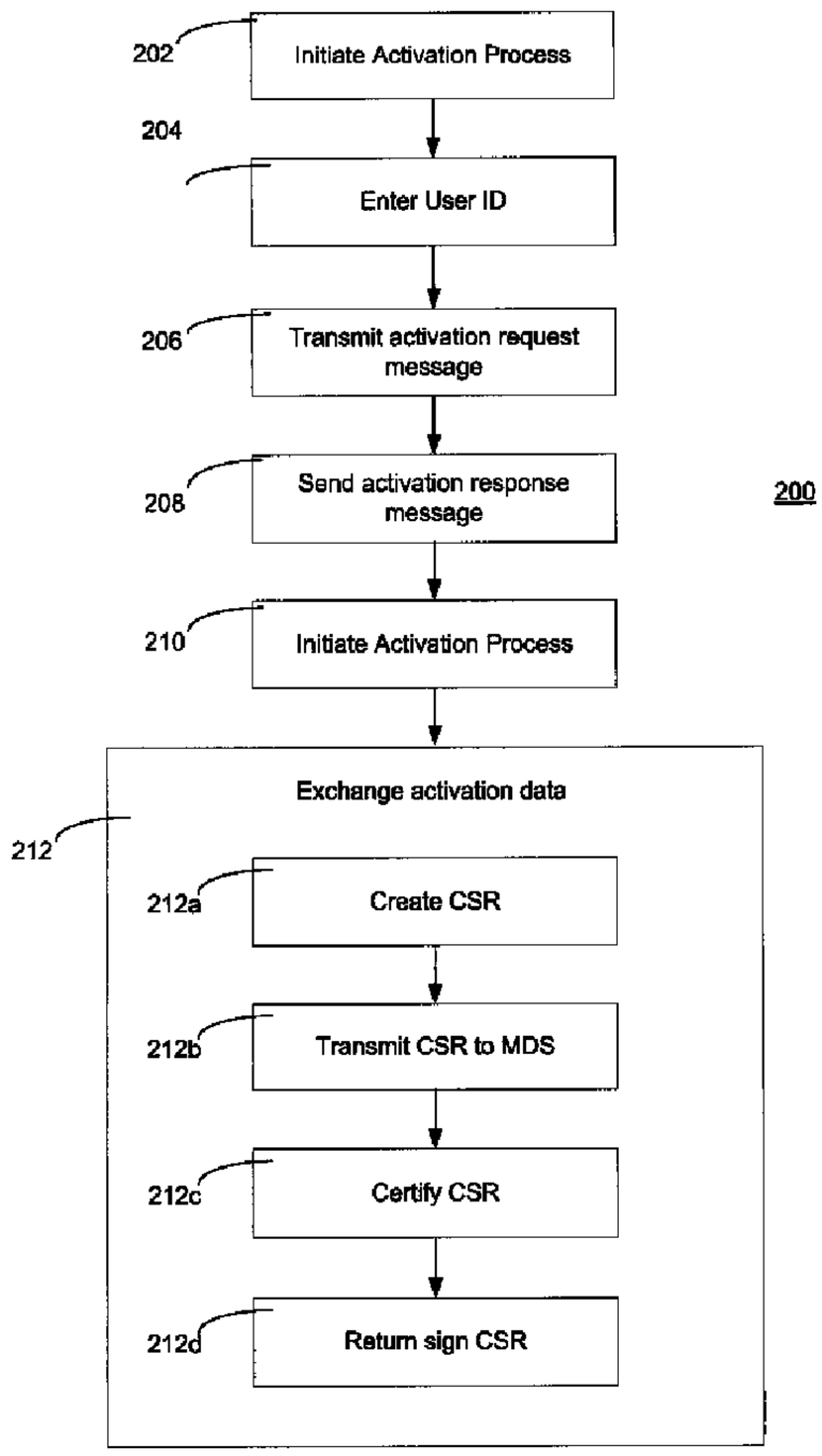
(51) Cl.Int./Int.Cl. *H04L 9/32* (2006.01),
H04L 9/30 (2006.01)

(72) Inventeurs/Inventors:
BROWN, MICHAEL K., CA;
BROWN, MICHAEL S., CA;
KIRKUP, MICHAEL, CA

(73) Propriétaire/Owner:
BLACKBERRY LIMITED, CA

(74) Agent: INTEGRAL IP

(54) Titre : SYSTEME ET METHODE DE FOURNITURE DE CERTIFICATS POUR DISPOSITIFS
(54) Title: SYSTEM AND METHOD FOR PROVISIONING DEVICE CERTIFICATES



(57) Abrégé/Abstract:
A method is provided for provisioning a device certificate on a device. The device is configured to communicate wirelessly with a plurality of backend servers via a communication network. The communication network includes a mobile data server. An activation

CA 2593888 C 2014/09/09

(11)(21) 2 593 888

(13) C

(57) Abrégé(suite)/Abstract(continued):
request is initiated to the mobile data server for activating the device on the communication network. During activation, a device certificate request is provided to the mobile data server for the device. The device certificate request includes at least a user identifier, a device identifier and a device public key. The device certificate request is forwarded from the mobile data server to a predefined certification authority. A device certificate from the predefined certification authority is received at the device in response to the device certificate request.

ABSTRACT

A method is provided for provisioning a device certificate on a device. The device is configured to communicate wirelessly with a plurality of backend servers via a communication network. The communication network includes a mobile data server. An activation request is initiated to the mobile data server for activating the device on the communication network. During activation, a device certificate request is provided to the mobile data server for the device. The device certificate request includes at least a user identifier, a device identifier and a device public key. The device certificate request is forwarded from the mobile data server to a predefined certification authority. A device certificate from the predefined certification authority is received at the device in response to the device certificate request.

SYSTEM AND METHOD FOR PROVISIONING DEVICE CERTIFICATES

[0001] The present invention relates generally to digital security and specifically to a system and method for provisioning device certificates.

[0002] The continued growth of telecommunication networks has led to the proliferation of communication devices that are used for the transfer of both voice and data. Personal Digital Assistants (PDAs) and smart-phones are examples of wireless communication devices that enable users to communicate via voice communications, electronic mail (e-mail), Short Message Service (SMS) messages as well as instant messaging. Additionally, many of these devices also include Web browsers and other applications to provide the users with information and access to remote data.

[0003] Due to their portability and ever-increasing functionality, wireless communication devices are becoming a necessity in today's business environment. Conducting business on the Internet is often efficient and cost effective, particularly when products and services can be distributed electronically.

[0004] However, as more people have access to the network and more data becomes available on the network, the risk of the wrong people accessing sensitive data increases. Accordingly, it is desirable for many network administrators to limit the devices that can access their network. One mechanism for limiting such access is the use of device certificates.

[0005] A device certificate is defined as a public key certificate or an attribute certificate tying the identity of a device to its attributes. An example of the use of digital certificates is the Device Certificate Service provided by VeriSign®. The VeriSign® Device Certificate Service embeds X.509 certificates into hardware devices, which allows service providers to perform strong authentication of their devices. Device manufacturers order certificates in bulk by providing a list of Media Access Control (MAC) addresses or unique device identifiers for the certificates. The issued certificates are returned to the manufacturers, who can then incorporate the process of injecting the certificates into the target devices as part of its overall device manufacturing process.

[0006] However, the process of assigning digital certificates during manufacture places an unnecessary burden on the manufacturing process. Further, it limits the digital certificate to a single certifying authority, regardless of the device's purchaser.

[0007] U.S. Patent Application No. 11/002,315 filed by Tet Hin Yeap et al and titled "System and Method for Access Control" teaches a system for restricting access based on device certificates. In order to assign a certificate to a device, Yeap teaches a system administrator transmitting an email request. The email includes unique identifiers of both the device and an access server. Both identifiers are used to generate a certificate, which is transmitted to the device via an email.

[0008] However, the use of the access server identifier ties the device to a single access server. Further, the method requires an email from a system administrator to initiate the certificate. For application in less technically sophisticated companies, such a step would provide an unnecessary burden on the user.

[0009] Lastly, in a document titled "Step-by-Step Guide to Deploying Windows Mobile-based Devices with Microsoft Exchange Server 2003 SP2: Appendix A. Deploying Exchange ActiveSync with Certificate-Based Authentication" a method for certificate enrolment configuration is taught. The document teaches a system administrator configuring an Extensible Markup Language (XML) script for device certificate enrolment. The XML script is uploaded to Active Directory using Microsoft Visual Basic Scripting Edition (VBScript). Active Directory is a Microsoft® directory service provided by a network server that provides means to manage identities and relationships that make up a network environment. Accordingly, when a user "cradles" a device, it connects to a corporate network via software on the user's computer. At this point, the XML script created by the administrator is delivered to the device and the certificate enrolment can begin.

[0010] However, similar to the previously described solution, the solution presented by this document is difficult to implement. Further, it requires that the device be able to communicate with a server via a cradle arrangement. Such a set-up precludes wireless certificate registration.

[0011] Accordingly, there is a need for a method of provisioning device certificates that overcomes the limitations of the prior art.

GENERAL

[0012] A certificate creation request is preferably bootstrapped on to an activation process and generated by the device itself. During this process, the device preferably creates a certificate request in the form of a certificate service request. This certificate service

request preferably includes both a device identifier and a corresponding user's identifier to bind the two together.

[0013] In accordance with one embodiment there is preferably provided a method for provisioning a device certificate on a device configured to communicate wirelessly with a plurality of backend servers via a communication network including a mobile data server, the method comprising the steps of: initiating an activation request to the mobile data server for activating the device on the communication network; during activation of the device, providing a device certificate request to the mobile data server for the device, the device certificate request including at least a user identifier, a device identifier and a device public key, wherein the device certificate request is forwarded from the mobile data server to a predefined certification authority; and receiving a device certificate from the predefined certification authority in response to the device certificate request.

[0014] In accordance a further embodiment there is preferably provided a wireless communication device configured to: initiate an activation request to a mobile data server for activating the device on a communication network; during activation of the device, provide a device certificate request to the mobile data server for the device, the device certificate request including at least a user identifier, a device identifier and a device public key, wherein the device certificate request is forwarded from the mobile data server to a predefined certification authority; and receive a device certificate from the predefined certification authority in response to the device certificate request.

BRIEF DESCRIPTION OF THE DRAWINGS

[0015] Embodiments of the present invention will now be described by way of example only with reference to the following drawings in which:

Figure 1 is a block diagram illustrating a communication network infrastructure;

Figure 2 is a flow chart illustrating a device provisioning process; and

Figure 3 is a block diagram illustrating a mobile device.

DESCRIPTION OF PREFERRED EMBODIMENTS

[0016] For convenience, like numerals in the description refer to like structures in the drawings. Referring to Figure 1, a communication network infrastructure for a wireless communication device is illustrated generally by numeral 100. The communication infrastructure 100 comprises a plurality of communication devices 102, or simply devices

102, a communication network 104, , a certification authority (CA) 118 and a plurality of backend servers 108.

[0017] The devices 102 include wireless computing devices such as a smart phone, a personal digital assistant (PDA), and the like. The devices 102 are in communication with one or more of the backend servers 108 via the communication network 104. Accordingly, the communication network 104 may include several components such as a wireless network 110, a relay 112, a corporate server 114 and/or a mobile data server 116 for relaying data between the devices 102 and the backend servers 108. An example of a mobile data server 116 is the BlackBerry Enterprise Server provided by Research in Motion.

[0018] The backend servers 108 include servers such as a Web server 108a, an application server 108b, and an application server with web services. It will be appreciated by a person of ordinary skill in the art that the network architecture described herein is exemplary and that changes may be made to one or more components to accommodate different network configurations without affecting the scope of the invention described and claimed herein.

[0019] Referring to Figure 3, a typical device 102 is illustrated in more detail. The device 102 is often a two-way communication device having both voice and data communication capabilities, including the capability to communicate with other computer systems. Depending on the functionality provided by the device mobile, it may be referred to as a data messaging device, a two-way pager, a cellular telephone with data messaging capabilities, a wireless Internet appliance, or a data communication device such as a PDA (with or without telephony capabilities).

[0020] The device 102 includes a communication subsystem 311, which includes a receiver 312, a transmitter 314, and associated components, such as one or more embedded or internal antenna elements 316 and 318, local oscillators (LOs) 313, and a processing module such as a digital signal processor (DSP) 320. As will be apparent to those skilled in field of communications, the particular design of the communication subsystem 311 depends on the communication network in which device 102 is intended to operate.

[0021] The device 102 includes a microprocessor 338 which controls general operation of the device 102. The microprocessor 338 also interacts with additional device subsystems such as a display 322, a flash memory 324, a random access memory (RAM) 326,

auxiliary input/output (I/O) subsystems 328, a serial port 330, a keyboard 332, a speaker 334, a microphone 336, a short-range communications subsystem 340 such as Bluetooth™ for example, and any other device subsystems or peripheral devices generally designated at 342. Operating system software used by the microprocessor 338 is preferably stored in a persistent store such as the flash memory 324, which may alternatively be a read-only memory (ROM) or similar storage element (not shown). Those skilled in the art will appreciate that the operating system, specific device applications, or parts thereof, may be temporarily loaded into a volatile store such as RAM 326.

[0022] The microprocessor 338, in addition to its operating system functions, preferably enables execution of software applications on the device 102. A predetermined set of applications, which control basic device operations, is installed on the device 102 during its manufacture. These basic operations typically include data and voice communication applications, for example. Additionally, applications may also be loaded onto the device 102 through the communication network 104, an auxiliary I/O subsystem 328, serial port 330, short-range communications subsystem 340, or any other suitable subsystem 342, and installed by a user in RAM 326 or preferably a non-volatile store (not shown) for execution by the microprocessor 338. Such flexibility in application installation increases the functionality of the device 102 and may provide enhanced on-device features, communication-related features, or both.

[0023] The display 322 is used to visually present an application's graphical user interface (GUI) to the user. The user can manipulate application data by modifying information on the GUI using an input device such as the keyboard 332 for example. Depending on the type of device 102, the user may have access to other types of input devices, such as, for example, a scroll wheel, light pen or touch sensitive screen.

[0024] Before the user can use the device 102 to access the backend servers 108, an activation process registers the device 102 with the communication network 104. The activation process is an application executing on the device. The activation process may be part of the device operating system or an addition thereto. Referring to Figure 2, a flow diagram illustrating the activation process is illustrated generally by numeral 200.

[0025] In step 202, the activation process is initiated. In the present embodiment, the activation process is initiated by the user selecting an activation program on the device 102. However it will be appreciated that the activation process could be initiated by the device 102 itself upon startup or at a predetermined time, for example. Furthermore, the

activation process could be initiated by the user via a website using a pre-existing network connection, such as using a personal computer with Internet access for example.

[0026] Once the activation process is initiated, it continues at step 204. In step 204, the user is prompted to enter user identification. In the present embodiment, the user identification includes a pre-assigned electronic mail (email) address and an activation password. The activation password is established by a system administrator for the purpose of the activation process. In the present embodiment, the system administrator can be either a corporate Information Technology (IT) department or a service provider, depending on the implementation selected by the user.

[0027] In step 206, the device 102 transmits an activation request message to the mobile data server 116. The activation request message includes information about the device 102, such as routing information and the device's activation public keys, for example. In the present embodiment, this is achieved by transmitting an activation request email to the user's email account. The mobile data server 116 receives the activation request email en route and retrieves the information.

[0028] In step 208, the mobile data server 116 sends an activation response message to the device 102. The activation response message includes information about the mobile data server 116 such as routing information and the mobile data server's public keys, for example. In the present embodiment, this is achieved by transmitting an activation request email that is received by the device 102.

[0029] In step 210, the mobile data server 116 and the device 102 establish a master encryption key. Both the mobile data server 116 and the device 102 verify their knowledge of the master encryption key to each other. Generation and verification of such a master encryption key is beyond the scope of the present invention and it will be appreciated that any appropriate state-of-the-art or proprietary technique may be used.

[0030] One such technique is described in detail in Applicant's co-pending U.S. Application Serial No. 11/093,954, titled "Deploying and Provisioning Wireless Handheld Devices", and filed March 30, 2005. Using this technique, the user generates a long-term encryption key pair and a short-term authentication key pair. The authentication key pair is generated using a shared secret. In the present embodiment, the shared secret is the activation password. The public keys of both key pairs are used as the activation public keys.

[0031] Once the device's public keys are received by the mobile data server 116, the user is verified. Once the device 102 is verified, the mobile data server 116 generates its own short-term authentication key pair, also using the activation password. The mobile data server 116 also generates its own long-term encryption key pair. Using the public keys generated by the device 102 and the activation password, the mobile data server 116 generates a master encryption key. The activation password provides the authentication necessary to trust the information exchanged. The mobile data server's short-term public authentication key, long-term public encryption key, a key confirmation value calculated using the newly generated master encryption key, and a known string, are sent to the device 102.

[0032] The device 102 receives the information from the mobile data server 116 and generates the device's own master encryption key. With this master key the device 102 verifies the key confirmation value. For example, the key confirmation value could be the hash of the master key the known string, as agreed upon by the device 102 and the mobile data server 116. If the key confirmation value does not verify, the master key created by the device 102 is not trusted, and it is assumed that someone is trying to compromise the connection. If the master encryption key generated by the device 102 seems valid, the device 102 sends a final key confirmation value to the mobile data server 116. The mobile data server 116 receives the message, verifies the key confirmation value and marks the device 102 as ready to go. Therefore, it will be appreciated that a secure communications tunnel can be established between the requesting device 102 and the mobile data server 116, and therefore the CA 118, even before the activation process is completed.

[0033] At this point the user and the mobile data server have been verified and full data exchange can securely take place using the corresponding long-term encryption key as desired. Data exchange may comprise e-mail messages, hypertext transfer protocol (HTTP)-based traffic, such as extensible markup language (XML), wireless markup language (WML), or other forms of data. Accordingly, if the master encryption key confirmation succeeds, the activation process proceeds with further communication being encrypted as desired.

[0034] In step 212, the mobile data server 116 and device 102 exchange data to facilitate further communication between the device 102 and the communication network 104 as well as the backend servers 108. As part of this data exchange, the device 102 requests, and is assigned, a device certificate.

[0035] In step 212a, the device 102 creates a certificate request using a digital certificate protocol. In the present embodiment, the device 102 creates a certificate signing request (CSR) using the Public-Key Cryptography Standards No. 10 (PKCS10) protocol. The PKCS10 protocol is well known in the art and need not be described in detail. It was developed by RSA Laboratories and is described in a document titled "PKCS #10 v1.7: Certification Request Syntax Standard", dated May 26, 2000. Although PKCS10 is used to implement the CSR, any appropriate protocol may used, as will be appreciated by a person of ordinary skill in the art.

[0036] In accordance with the PKCS10 protocol, a CSR has the following syntax:

```
PKCSReq CertificationRequest ::= SEQUENCE {
        certificationRequestInfo SEQUENCE {
                version INTEGER,
                subject Name,
                subjectPublicKeyInfo SEQUENCE {
                        algorithm AlgorithmIdentifier,
                        subjectPublicKey BIT STRING
                        }
                attributes [0] Attributes{{ CRIAttributes }}
                }
        signatureAlgorithm AlgorithmIdentifier,
        signature BIT STRING
        }
```

[0037] Version is a version number of the PKCS10 protocol. It is used for compatibility with future revisions. Subject is the name of the certificate subject. SubjectPublicKeyInfo contains information about the public key being certified. The information identifies the entity's public-key algorithm and any associated parameters.

[0038] The attributes are a collection of data providing additional information about the subject of the certificate. More information about attribute types is provided in PKCS No. 9, developed by RSA Laboratories and described in a document titled "PKCS #9 v2.0: Selected Object Classes and Attribute Types", dated February 25, 2000. Alternately, the attributes may be locally defined. In accordance with the present embodiment, the attributes are used to transmit the user's email address as well as a personal identification

number (PIN) associated with the device 102 as part of the CSR. This act binds the two identifiers together.

[0039] In step 212b, the CSR is received by the mobile data server 116, which has a predefined certification authority (CA 118) associated with it. Often, the CA 118 is a third party such as VeriSign® or Entrust®, for example. However, the mobile data server 116 may also act as its own CA 118. In this manner, a company or organization could operate the CA 118.

[0040] In step 212c, the CSR is transmitted to the predefined CA 118 for certification. The CA 118 signs the CSR with its private key and the signed CSR becomes the device certificate. In step 212d, the device certificate is returned to the device 102 for future use, when required.

[0041] Once the device 102 has the device certificate at its disposal, the mobile data server 116 can use it to ensure that the device is allowed on the communication network 104. For example, if the user is fired or the device is compromised, the CA 118 can revoke the device certificate.

[0042] In general, a server or user manually checks to see if a device certificate has been revoked. This can be accomplished either by checking a Certificate Revocation List (CRL) that is published by the CA 118 by making an Online Certificate Status Protocol (OCSP) request. Accordingly, in order to check the status of a device certificate the mobile data server 116 can periodically make OCSP requests or check the CA's CRL.

[0043] After determining that a certificate has been revoked, the mobile data server 116 can automatically send a Kill command to the device 102 to disable it. The use of the device certificate helps to reduce the chance of activating the Kill command on the wrong device.

[0044] Alternately, the mobile data server 116 could refrain from forwarding traffic to and/or from the device 102 in the event that the digital certificate has been revoked. Therefore, it also reduces the chance of having an unwanted device on the network.

[0045] Accordingly, it will be seen that the embodiment described above provides a relatively simple method for obtaining a device certificate for a wireless device. Moreover, the device certificate is obtained when the device is provisioned on the communication network 104, thus limiting fraudulent use of the devices 102 and access to sensitive data on one or more of the backend servers 108.

[0046] Although the embodiment described describes a specific implementation, a person of ordinary skill in the art will appreciate that other embodiments may also be realized.

[0047] For example, in the embodiment described above, the activation request message is an email. However, other forms of messaging may also be used successfully. For example, a custom handshaking protocol may be implemented or an alternate messaging protocol, such as Short Messaging Service (SMS) may be used.

[0048] Further, although the previous embodiment describes using an email address to identify the user and a PIN to identify the device 102, other parameters may be used. For the user, sufficient information to uniquely identify him or her is desired. Therefore, a social insurance number may suffice. Other information like name, address, telephone number, employer and the like, or any combination thereof, may also be sufficient to identify the user as required.

[0049] Similarly, rather than use the PIN to identify the device 102, other information such as a serial number, a mobile identification number (MIN), or International Mobile Subscriber Identity (IMSI), for example, may be used. Such information may be used alone, or in combination, as required.

[0050] In the embodiments described above, the mobile data server 116 polls the CA 118 to determine the status of a device certificate. In an alternate embodiment, the CA 118 transmits a notification to the mobile data server 116 when the certificate is revoked. In such an embodiment, the CA 118 maintains a correlation between the mobile data server 116 and the device certificate when the CSR is submitted.

[0051] In all of the embodiments described above, generation of a device certificate is a dynamic operation that takes place during the activation of the device. A further benefit of this arranged is realized when the system administrator has established its own CA 118. In this case, their own CA 118 can issue the device certificates. This feature increases the amount of trust the system administrator has in the device certificate process.

[0052] Further, although the invention has been described with reference to certain specific embodiments, various modifications thereof will be apparent to those skilled in the art without departing from the spirit and scope of the invention as defined by the appended claims.

What is claimed is:

1. A method for provisioning a device certificate on a device configurable to communicate wirelessly with one or more backend servers via a communication network, the method comprising:

transmitting to a server in the communication network an activation request for activating the device on the communication network;

during activation of the device, transmitting, from the device to the server, a device certificate request for the device, the device certificate request comprising at least a user identifier and a device identifier; and

receiving at the device, from the server, a device certificate that comprises a signed version of the device certificate request, the signed version of the device request having been generated using a private key of a predefined certification authority, such that the device certificate binds together the user identifier and the device identifier.

2. The method of claim 1, wherein the user identifier is an email address.

3. The method of claim 1 or claim 2, wherein the device identifier is a device personal identification number or a device serial number or a device International Mobile Subscriber Identity (IMSI).

4. The method of any one of claims 1 to 3, wherein the device certificate request is in the form of a Public-Key Cryptography Standards No. 10 certificate signing request.

5. The method of any one of claims 1 to 4, wherein the predefined certification authority is maintained by the server in the communication network or is a third party certification authority or is maintained by an administrator of the server in the communication network.

6. The method of any one of claims 1 to 5, further comprising the step of establishing a secure communications tunnel between the device and the server in the communication network before requesting the device certificate.

7. The method of claim 6, wherein the device and the server each generate and exchange a pair of public encryption keys.

8. The method of claim 7, wherein the device and the server each use the public encryption key pairs and a shared secret to generate and verify a master encryption key.

9. The method of claim 8, wherein the shared secret is an authentication password.

10. A method for provisioning a device certificate on a device configurable to communicate wirelessly with one or more backend servers via a communication network comprising a server, the method comprising the steps of:

obtaining at the server an activation request for activating the device on the communication network;

during activation of the device, receiving at the server, from the device, a device certificate request for the device, the device certificate request comprising at least a user identifier and a device identifier; and

providing to the device, from the server, a device certificate that comprises a signed version of the device certificate request, the signed version of the device certificate request having been generated using a private key of a predefined certification authority, such that the device certificate binds together the user identifier and the device identifier.

11. A wireless communication device comprising:

means for transmitting to a server of a communication network an activation request for activating the device on the communication network;

means for transmitting, from the device to the server, a device certificate request for the device during activation of the device, the device certificate request comprising at least a user identifier and a device identifier; and

means for receiving at the device, from the server, a device certificate that comprises a signed version of the device certificate request, the signed version of the device certificate request having been generated using a private key of a predefined certification authority, such that the device certificate binds together the user identifier and the device identifier.

12. The device of claim 11, wherein the user identifier is an email address.

13. The device of claim 11 or 12, wherein the device identifier is a device personal identification number or is a device serial number or is a device International Mobile Subscriber Identity (IMSI).

14. The device of any one of claims 11 to 13, wherein the device certificate request is in the form of a Public-Key Cryptography Standards No. 10 certificate signing request.

15. The device of any one of claims 11 to 14, wherein the predefined certification authority is maintained by the server in the communication network or is a third party certification authority or is maintained by an administrator of the server in the communication network.

16. The device of any one of claims 11 to 15, further configured to establish a secure communications tunnel with the server in the communication network before requesting the device certificate.

17. The device of claim 16, wherein the device is configured to generate and exchange a pair of public encryption keys with the server.

18. The device of claim 17, wherein the device is configured to use the public encryption key pairs and a shared secret to generate and verify a master encryption key.

19. The device of claim 18, wherein the shared secret is an authentication password.

20. A computer program product for provisioning a device certificate on a device configurable to communicate wirelessly with one or more backend servers via a communication network, the computer program product comprising instructions stored in a memory of the device, which, when executed on a processor of the device, cause the device to implement the method of any one of claims 1 to 9.

21. A method at a communication device for provisioning a device certificate, the method comprising:

transmitting a device certificate request to a server in a communication network using an established communications channel between the communication device and the server, wherein the device certificate request comprises at least a user identifier and a device identifier; and

in response to transmitting the device certificate request, receiving a device certificate that includes the user identifier and the device identifier and that is signed by a private key of a certification authority.

22. The method of claim 21, further comprising:

enabling user input of the user identifier at the communication device.

23. The method of claim 21 or claim 22, wherein the device certificate request is transmitted to the server in a communication that is encrypted with a master communication key established between the server and the communication device.

24. The method of claim 23, wherein the device certificate is received from the server in a communication that is encrypted with the master communication key.

25. The method of any one of claims 21 to 24, wherein the server acts as the certification authority.

26. The method of any one of claims 21 to 24, wherein the certification authority is a third party certification authority.

27. The method of any one of claims 21 to 26, wherein the user identifier is associated with a person and comprises one or more of the following: a number assigned by a government agency to the person, an identification of an employer of the person, a name or address or both of the person, a telephone number of the person.

28. The method of any one of claims 21 to 27, wherein the device identifier comprises one or more of the following: a device personal identification number, a device serial number, and a device International Mobile Subscriber Identity (IMSI).

29. A communication device configured:

to establish a master communication key with a server in a communication network for encryption and decryption of communication with the server;

to transmit a device certificate request to a server in a communication network using an established communications channel between the communication device and the server, wherein the device certificate request comprises at least a user identifier and a device identifier; and

in response to transmitting the device certificate request, to receive a device certificate that includes the user identifier and the device identifier and that is signed by a private key of a certification authority.

30. The communication device of claim 29, further configured to:

enable user input of the user identifier at the communication device.

31. The communication device of claim 29 or claim 30, wherein the device certificate request is transmitted to the server in a communication that is encrypted with a master communication key established between the server and the communication device.

32. The communication device of claim 31, wherein the device certificate is received from the server in a communication that is encrypted with the master communication key.

33. The communication device of any one of claims 29 to 32, wherein the server acts as the certification authority.

34. The communication device of any one of claims 29 to 32, wherein the certification authority is a third party certification authority.

35. The communication device of any one of claims 29 to 34, wherein the user identifier is associated with a person and comprises one or more of the following: a number assigned by a

government agency to the person, an identification of an employer of the person, a name or address or both of the person, a telephone number of the person.

36. The communication device of any one of claims 29 to 35, wherein the device identifier comprises one or more of the following: a device personal identification number, a device serial number, and a device International Mobile Subscriber Identity (IMSI).

37. A method at a server in a communication network, the method comprising:

receiving a device certificate request from a communication device over an established communications channel between the communication device and the server, wherein the device certificate request comprises at least a user identifier and a device identifier; and

responsive to receiving the device certificate request, providing to the communication device a device certificate that includes the user identifier and the device identifier and that is signed by a private key of a certification authority.

38. The method as recited in claim 37, wherein the device certificate request is received by the server in a communication that is encrypted with a master communication key established between the server and the communication device.

39. The method as recited in claim 38, wherein the device certificate is provided to the communication device by the server in a communication that is encrypted with the master communication key.

40. The method as recited in any one of claims 37 to 39, wherein the server acts as the certification authority.

41. The method as recited in any one of claims 37 to 39, wherein the certification authority is a third party certification authority.

42. The method as recited in any one of claims 37 to 41, wherein the user identifier is associated with a person and comprises one or more of the following: a number assigned by a government agency to the person, an identification of an employer of the person, a name or address or both of the person, a telephone number of the person.

43. The method as recited in any one of claims 37 to 42, wherein the device identifier comprises one or more of the following: a device personal identification number, a device serial number, and a device International Mobile Subscriber Identity (IMSI).

44. A server configured:

to receive a device certificate request from a communication device over an established communications channel between the communication device and the server, wherein the device certificate request comprises at least a user identifier and a device identifier; and

responsive to receiving the device certificate request, to provide to the communication device a device certificate that includes the user identifier and the device identifier and that is signed by a private key of a certification authority.

45. The server as recited in claim 44, wherein the device certificate request is received by the server in a communication that is encrypted with a master communication key established between the server and the communication device.

46. The server as recited in claim 45, wherein the device certificate is provided to the communication device by the server in a communication that is encrypted with the master communication key.

47. The server as recited in any one of claims 44 to 46, wherein the server acts as the certification authority.

48. The server as recited in any one of claims 44 to 46, wherein the certification authority is a third party certification authority.

49. The server as recited in any one of claims 44 to 48, wherein the user identifier is associated with a person and comprises one or more of the following: a number assigned by a government agency to the person, an identification of an employer of the person, a name or address or both of the person, a telephone number of the person.

50. The server as recited in any one of claims 44 to 49, wherein the device identifier comprises one or more of the following: a device personal identification number, a device serial number, and a device International Mobile Subscriber Identity (IMSI).

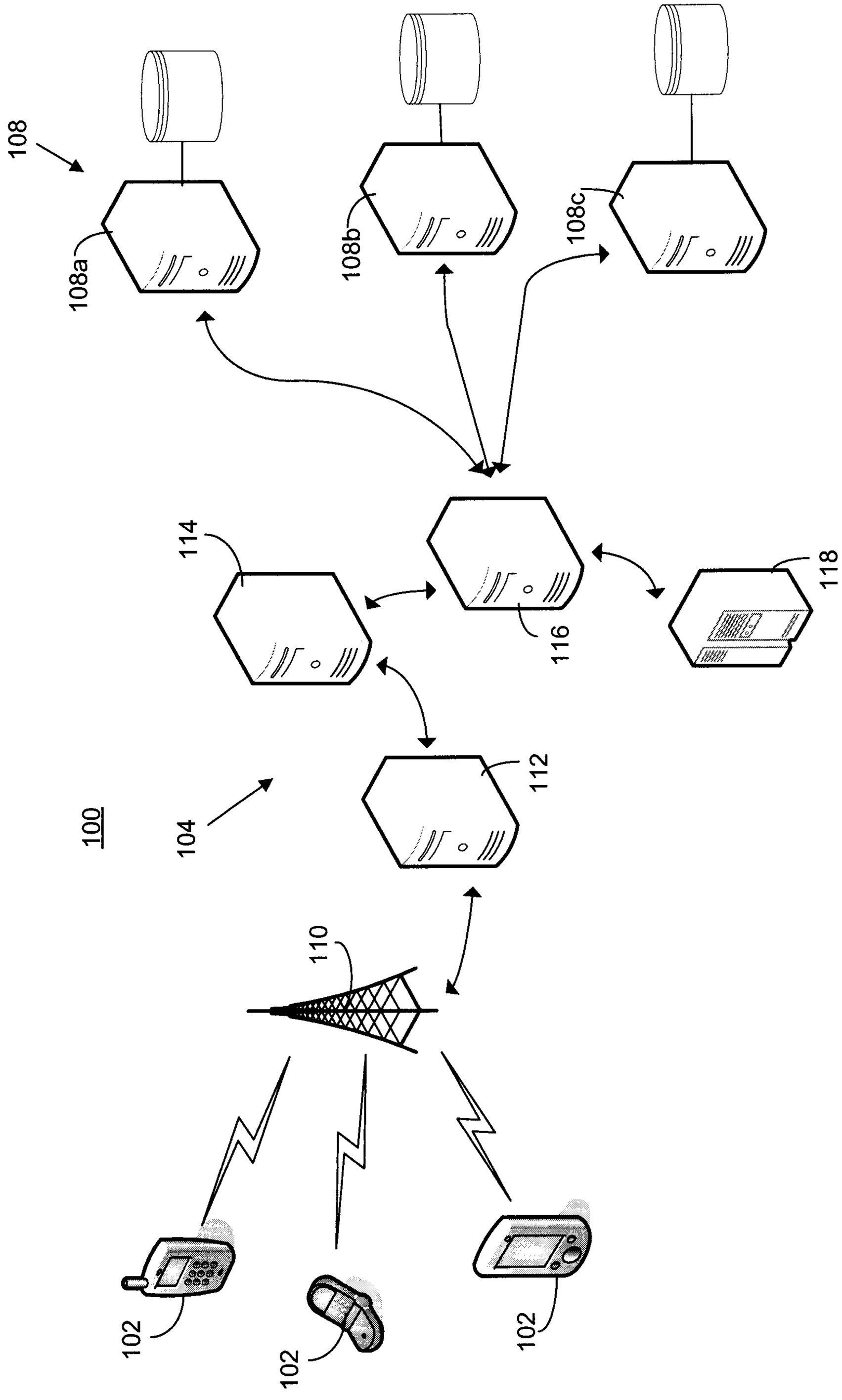


Figure 1

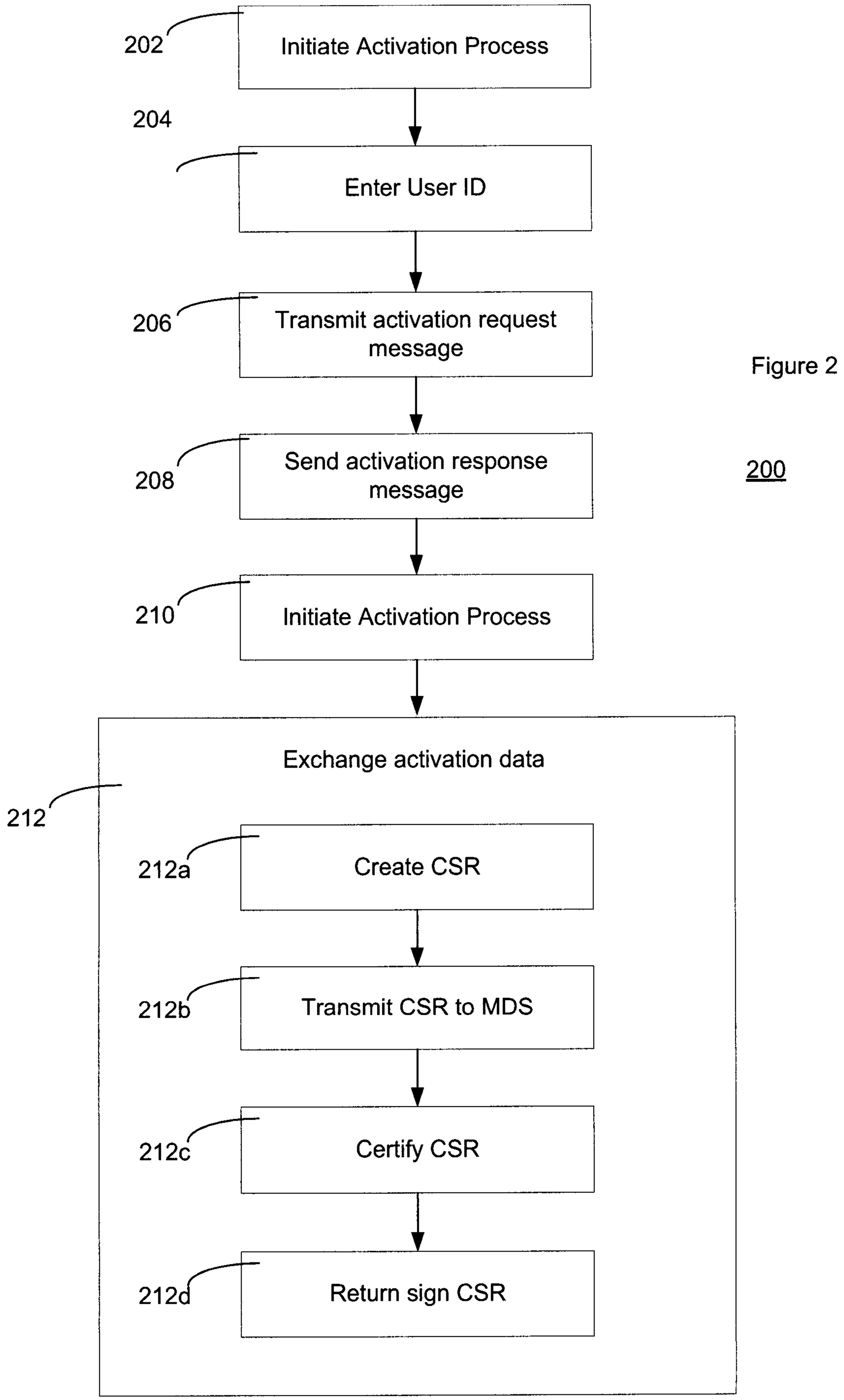

202
Initiate Activation Process
204
Enter User ID
206
Transmit activation request message
208
Send activation response message
210
Initiate Activation Process
Exchange activation data
212
212a
Create CSR
212b
Transmit CSR to MDS
212c
Certify CSR
212d
Return sign CSR

Figure 2

200

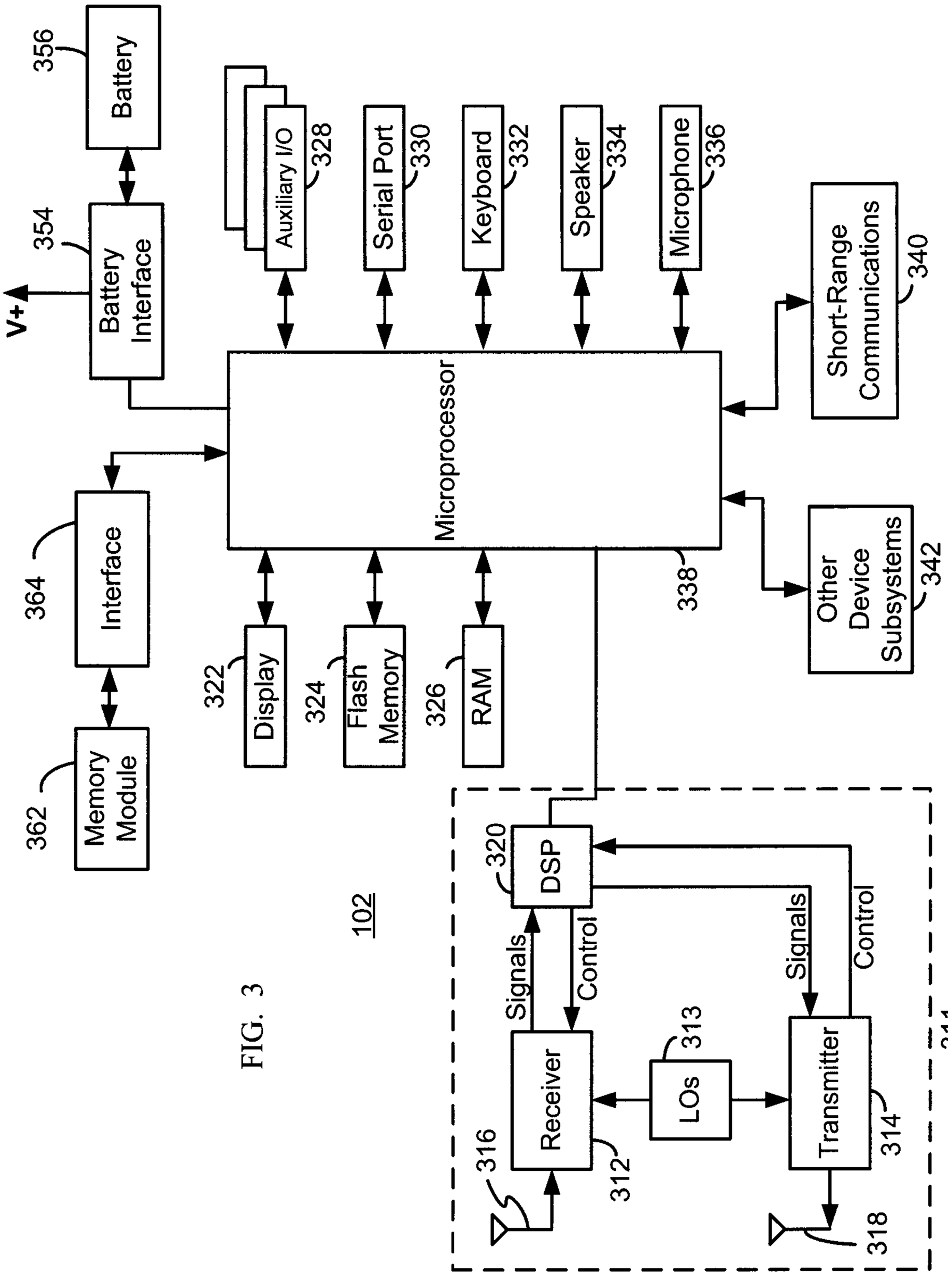
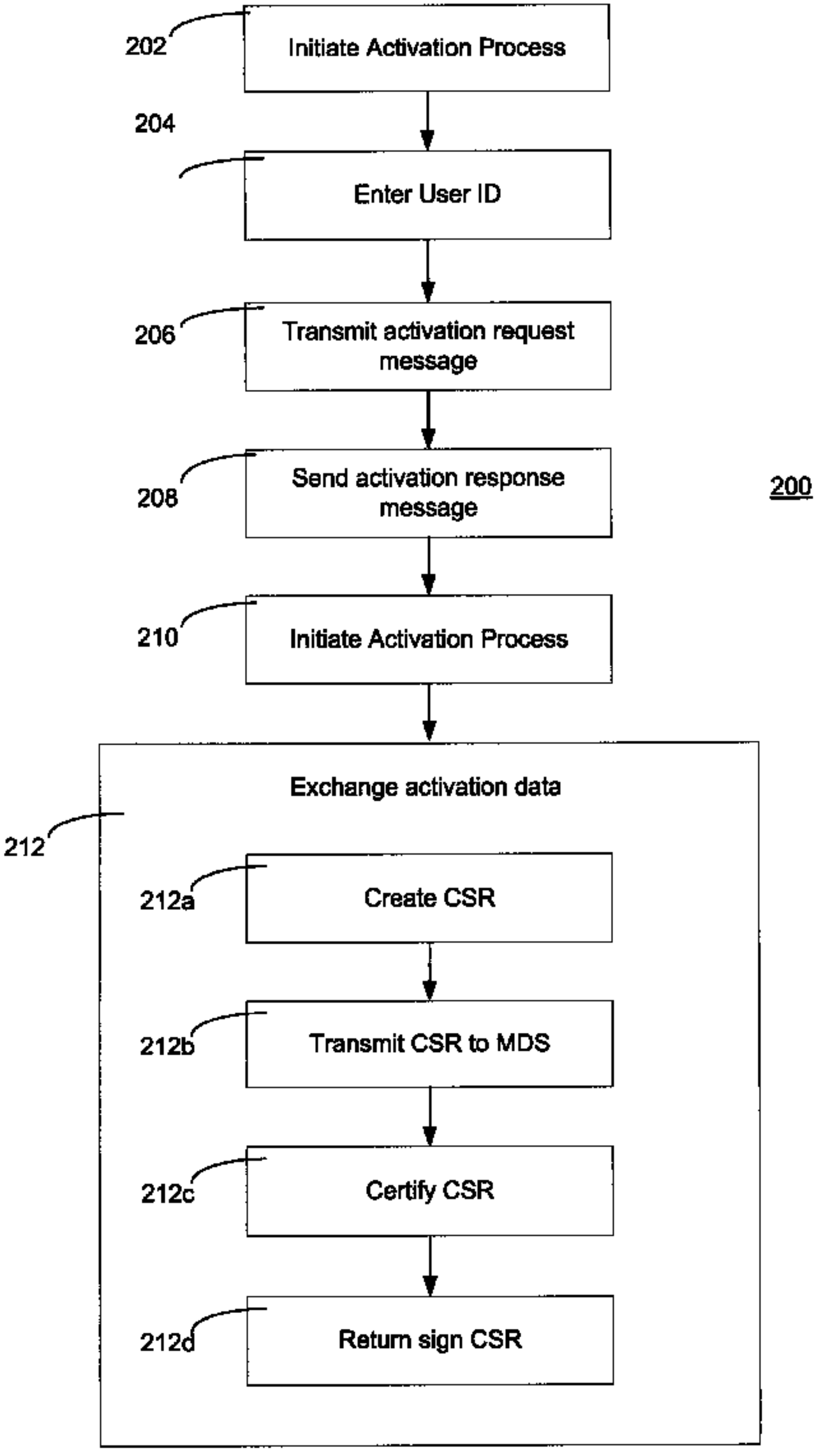

356
Battery
354
Battery Interface
V+
364
Interface
362
Memory Module
Auxiliary I/O
328
Serial Port
330
Keyboard
332
Speaker
334
Microphone
336
Microprocessor
338
Short-Range Communications
340
Other Device Subsystems
342
322
Display
324
Flash Memory
326
RAM
102
320
DSP
Signals
Control
Signals
Control
313
LOs
316
Receiver
312
Transmitter
314
318
311

FIG. 3


202
Initiate Activation Process
204
Enter User ID
206
Transmit activation request message
208
Send activation response message
200
210
Initiate Activation Process
Exchange activation data
212
212a
Create CSR
212b
Transmit CSR to MDS
212c
Certify CSR
212d
Return sign CSR