US 20070136098A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2007/0136098 A1

Smythe et al. (43) Pub. Date: Jun. 14, 2007

(54) SYSTEM AND METHOD FOR PROVIDING A SECURE FEATURE SET DISTRIBUTION INFRASTRUCTURE FOR MEDICAL DEVICE MANAGEMENT

(76) Inventors: **Alan H. Smythe**, White Bear Lake, MN (US); **Howard D. Simms**, Shoreview, MN (US); **Kenneth P. Hoyme**, Plymouth, MN (US); **George D. Jelatis**, Minneapolis, MN (US)

Correspondence Address:
CASCADIA INTELLECTUAL PROPERTY
500 UNION STREET
STE.1005
SEATTLE, WA 98101 (US)

(21) Appl. No.: **11/299,980**

(22) Filed: **Dec. 12, 2005**

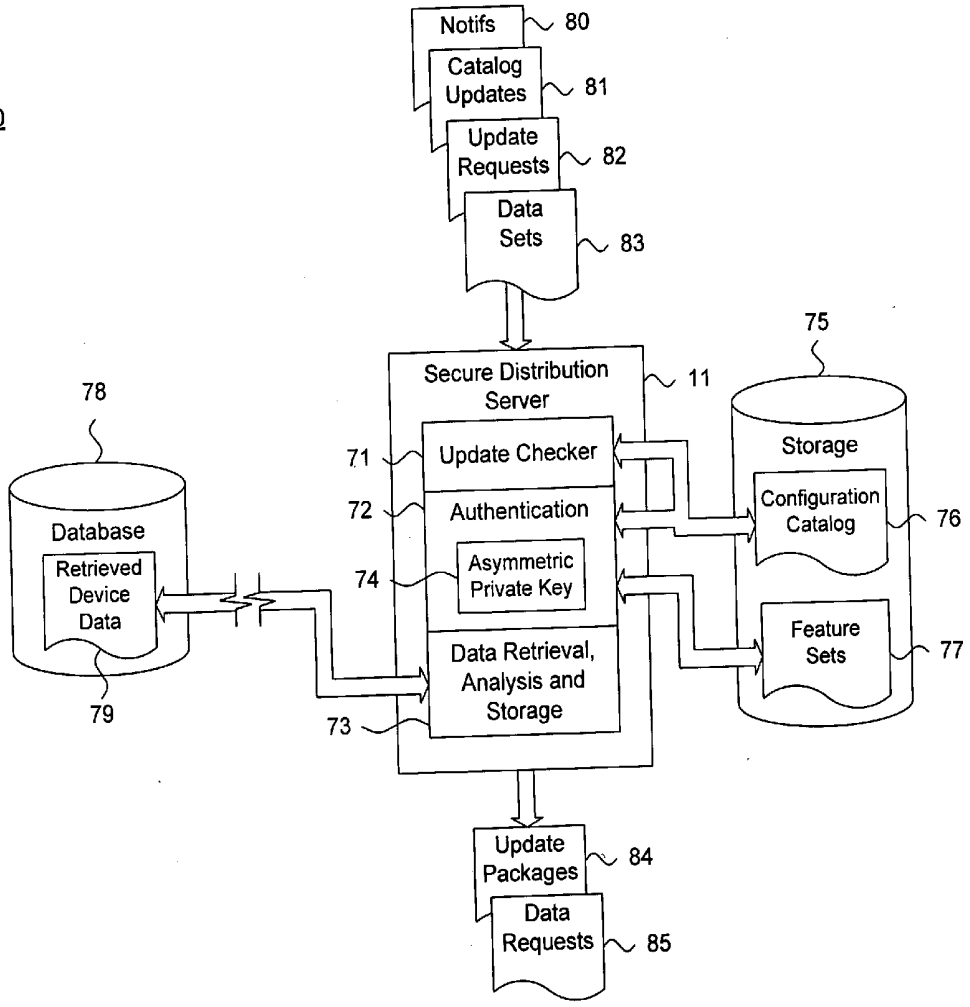
Publication Classification

(51) **Int. Cl.**
A61B 5/00 (2006.01)
G06F 19/00 (2006.01)
G06F 12/14 (2006.01)
G06F 15/173 (2006.01)

(52) **U.S. Cl.** **705/3**; 600/301; 709/225; 726/21

(57) **ABSTRACT**

A system and method for providing a secure feature set distribution infrastructure for medical device management is presented. A unique association is mapped for data download between a medical device and a communications device transiently coupleable to the medical device. A configuration catalog is maintained, including operational characteristics of at least one of the medical device and the communications device. The operational characteristics as maintained in the configuration catalog are periodically checked against a database storing downloadable sets of features and one or more feature sets including changed operational characteristics are identified for distribution. The one or more feature sets are digitally signed and the one or more feature sets are provided to the communications device over a plurality of networks. The one or more feature sets are authenticated and their integrity is checked over a chain of trust originating with a trusted source and terminating at the communications device.



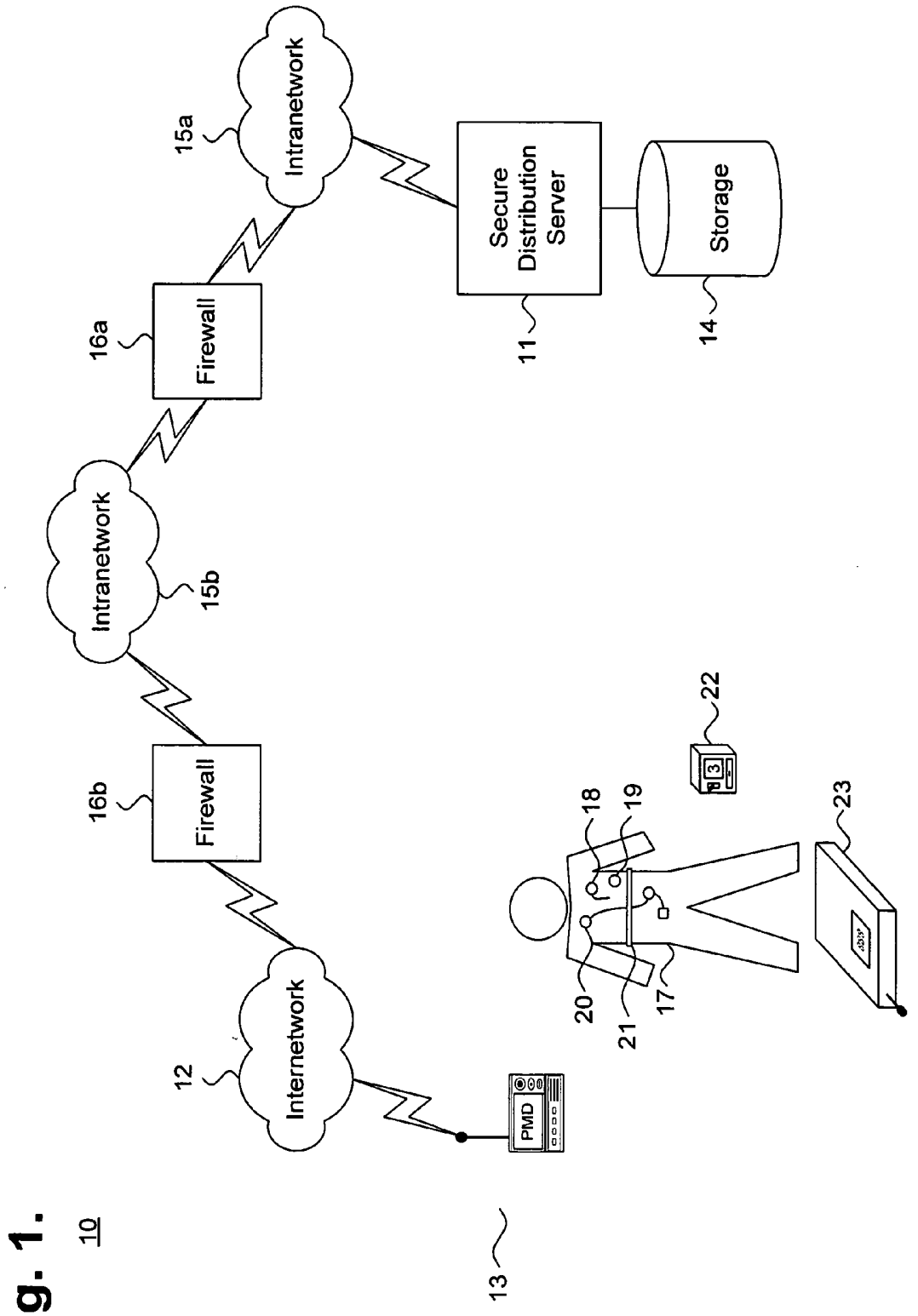

Intranetwork
15a
Secure Distribution Server
Storage
11
14
16a
Firewall
Intranetwork
15b
16b
Firewall
22
18
19
23
20
21
17
Internetwork
12
PMD
13
10

Fig. 1.

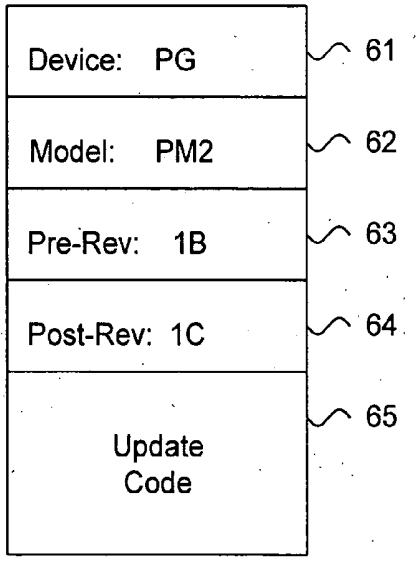
Fig. 2.

40

Device	Model	Serial No.	Rev.	PMD	Model	Serial No.	Rev
PG	PM2	45457	1A	RP	AB1	387	1B
41	42	43	44	45	46	47	48

Fig. 3.

60



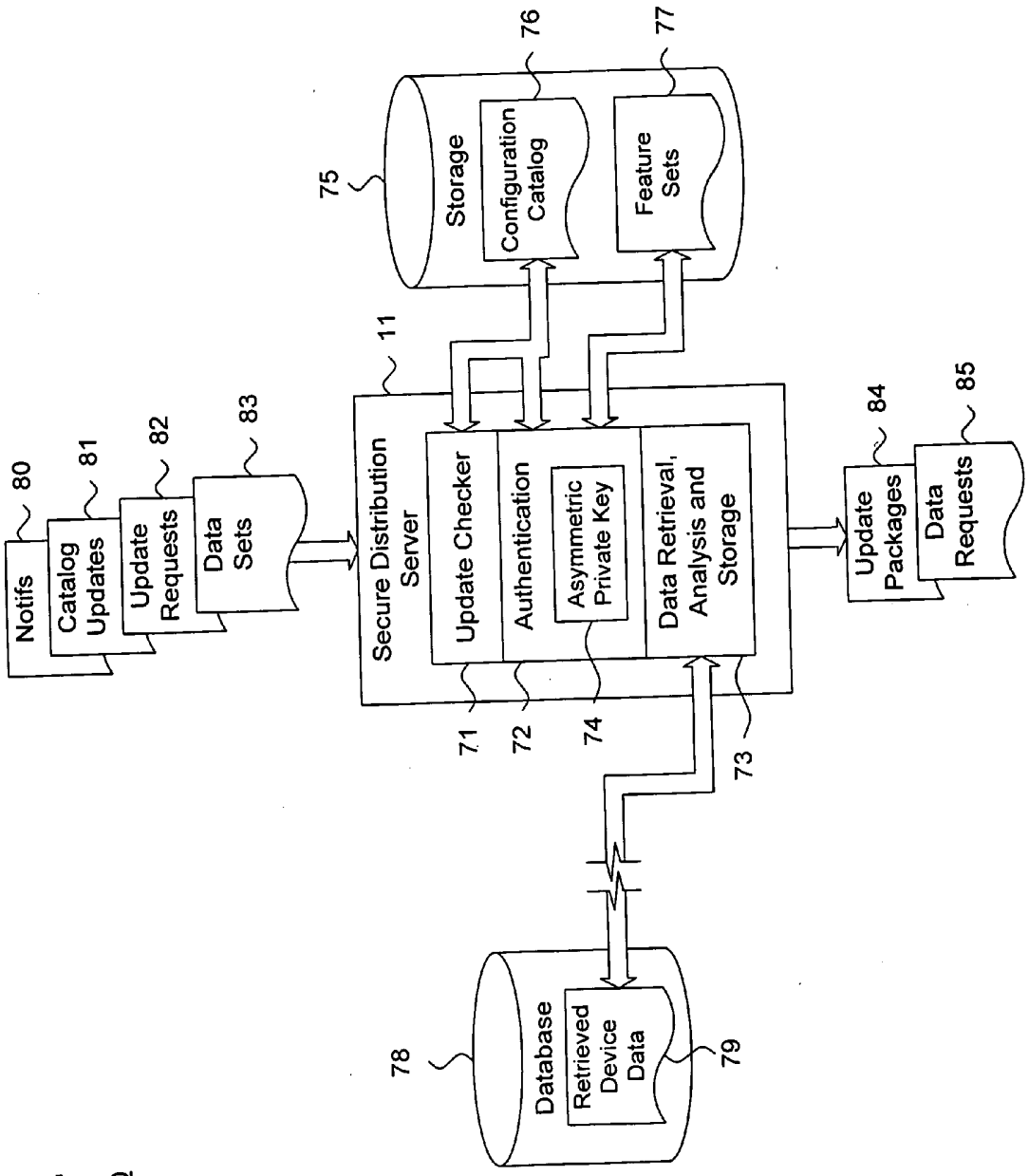

70
Notifs
80
Catalog Updates
81
Update Requests
82
Data Sets
83
Secure Distribution Server
11
Update Checker
71
Authentication
72
Asymmetric Private Key
74
Data Retrieval, Analysis and Storage
73
Storage
75
Configuration Catalog
76
Feature Sets
77
Update Packages
84
Data Requests
85
Database
78
Retrieved Device Data
79

Fig. 4.

Fig. 5A.

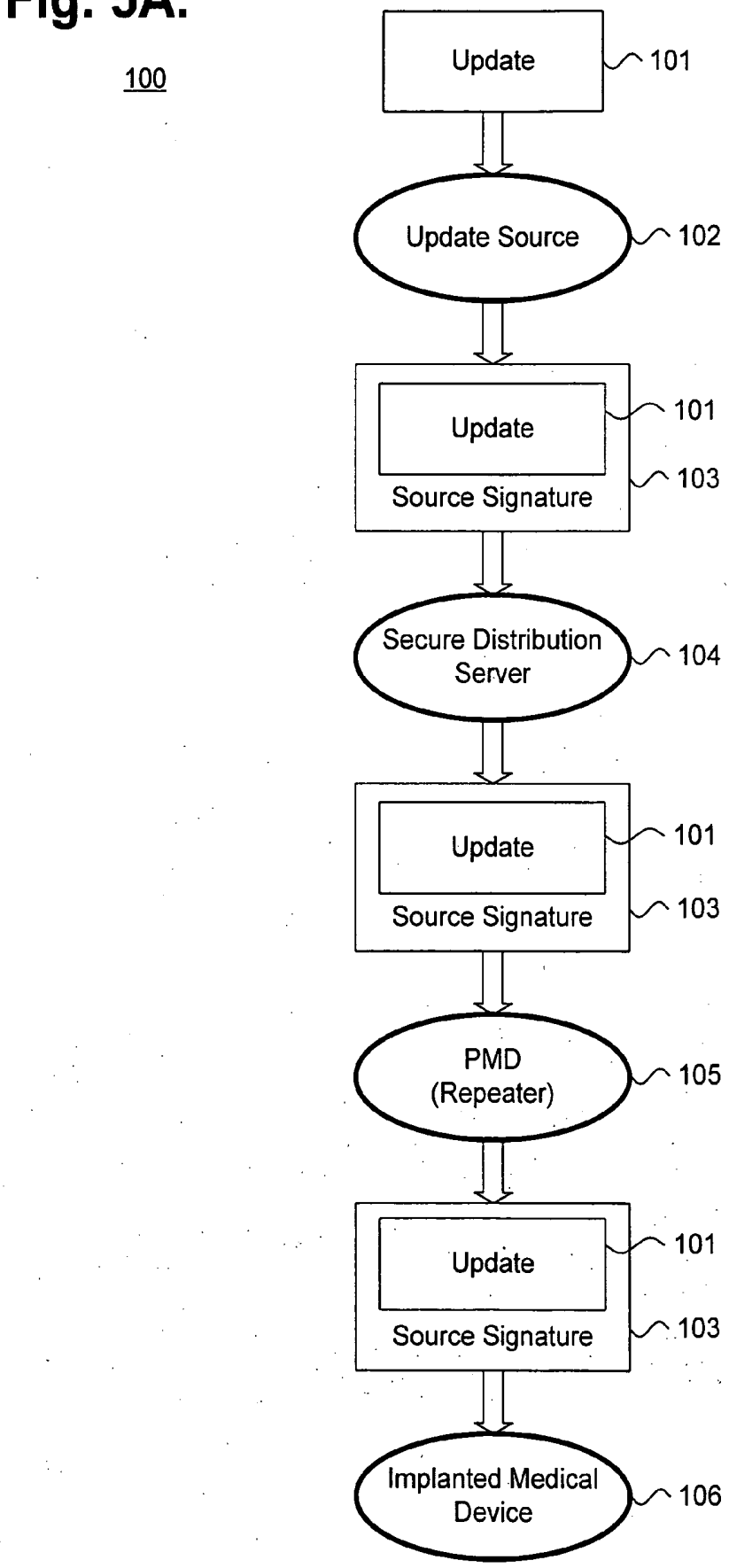

100
Update
101
Update Source
102
Update
101
Source Signature
103
Secure Distribution Server
104
Update
101
Source Signature
103
PMD (Repeater)
105
Update
101
Source Signature
103
Implanted Medical Device
106

Fig. 5B.

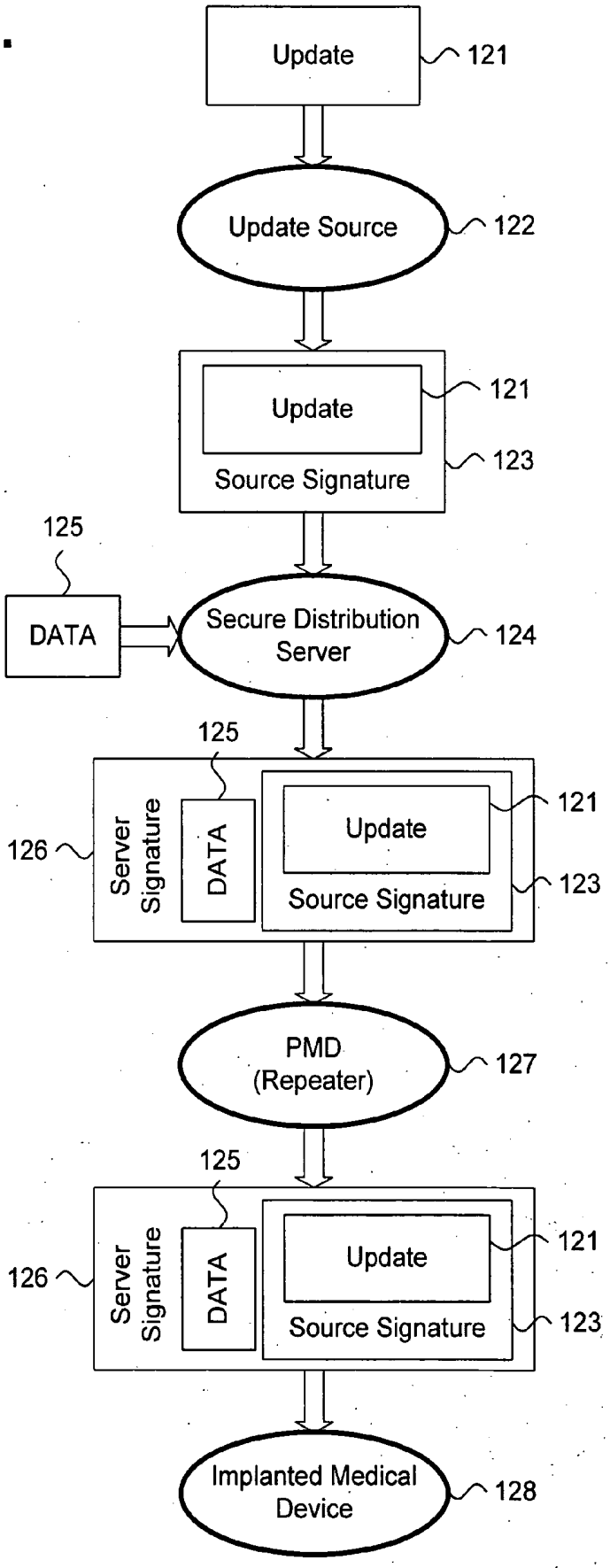

120
Update
121
Update Source
122
Update
121
Source Signature
123
125
DATA
Secure Distribution Server
124
125
126
Server Signature
DATA
Update
121
Source Signature
123
PMD (Repeater)
127
125
126
Server Signature
DATA
Update
121
Source Signature
123
Implanted Medical Device
128

Fig. 6.

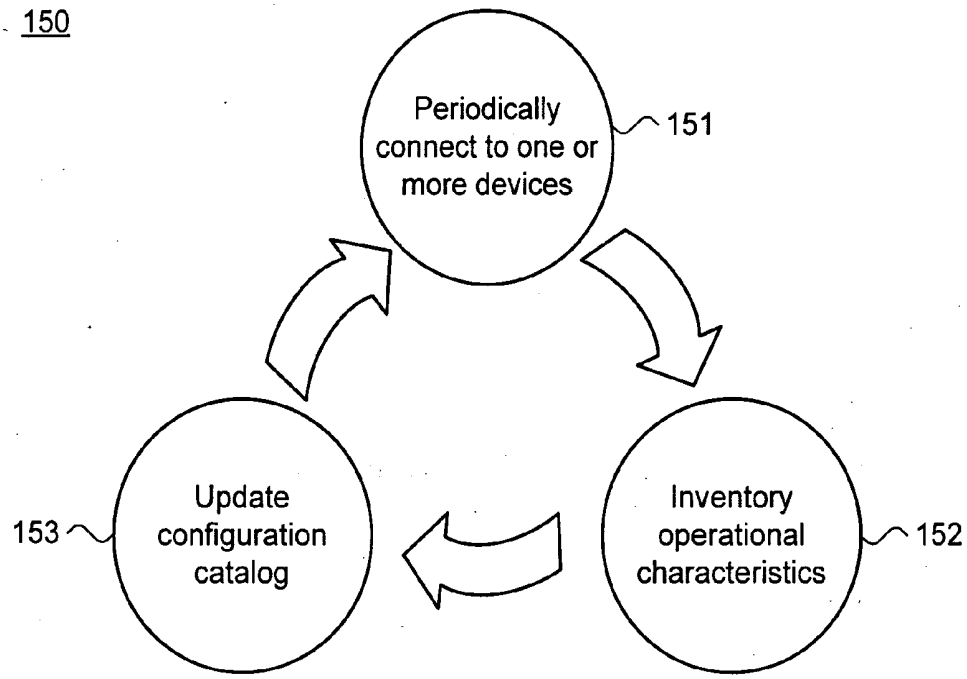

150
Periodically connect to one or more devices
151
Inventory operational characteristics
152
Update configuration catalog
153

Fig. 7.

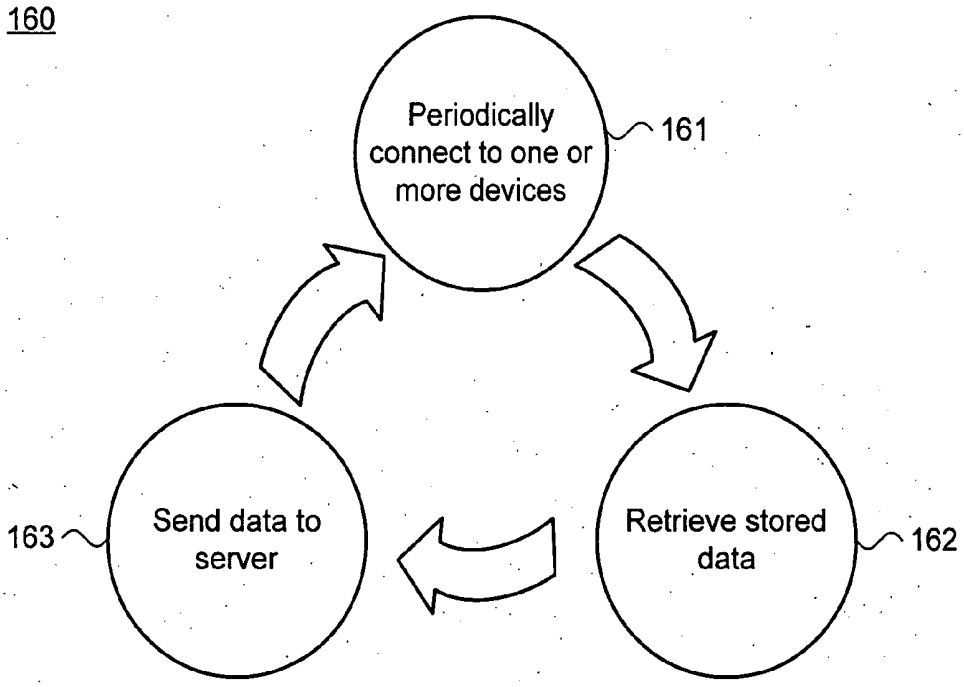

160
Periodically connect to one or more devices
161
Retrieve stored data
162
Send data to server
163

Fig. 8.

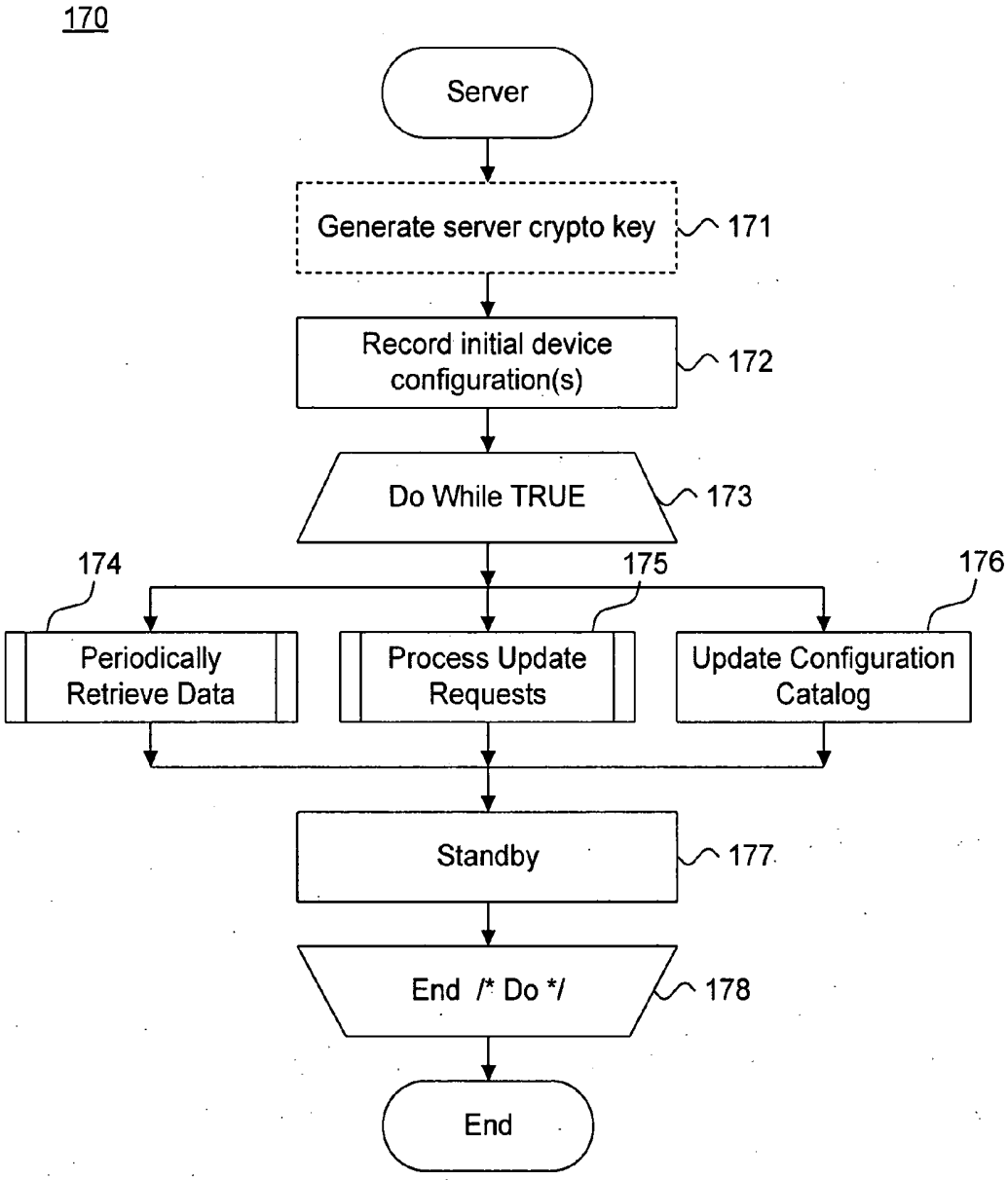

170
Server
Generate server crypto key
171
Record initial device configuration(s)
172
Do While TRUE
173
174
175
176
Periodically Retrieve Data
Process Update Requests
Update Configuration Catalog
Standby
177
End /* Do */
178
End

Fig. 9.

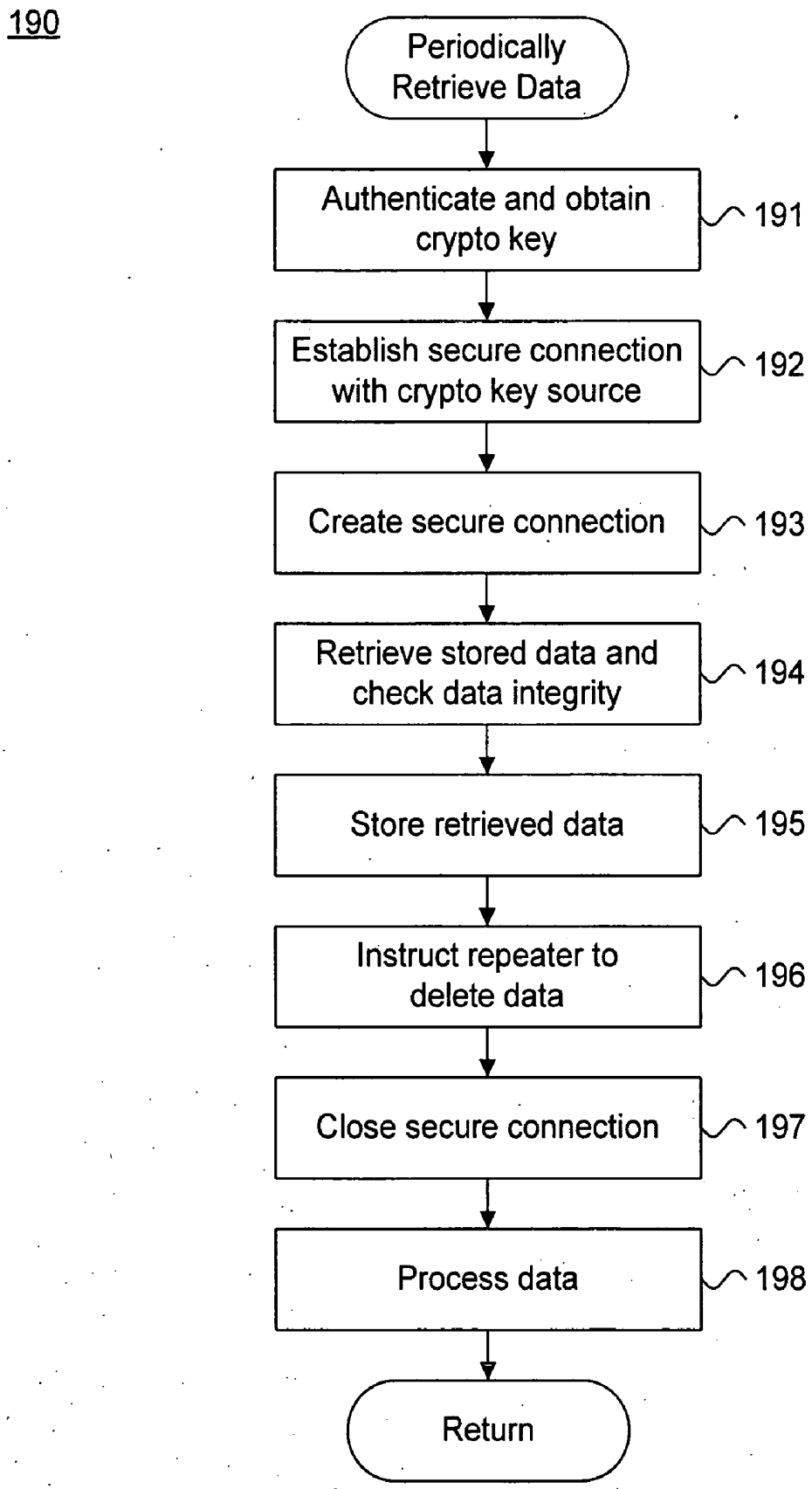

190
Periodically Retrieve Data
Authenticate and obtain crypto key
191
Establish secure connection with crypto key source
192
Create secure connection
193
Retrieve stored data and check data integrity
194
Store retrieved data
195
Instruct repeater to delete data
196
Close secure connection
197
Process data
198
Return

Fig. 10.

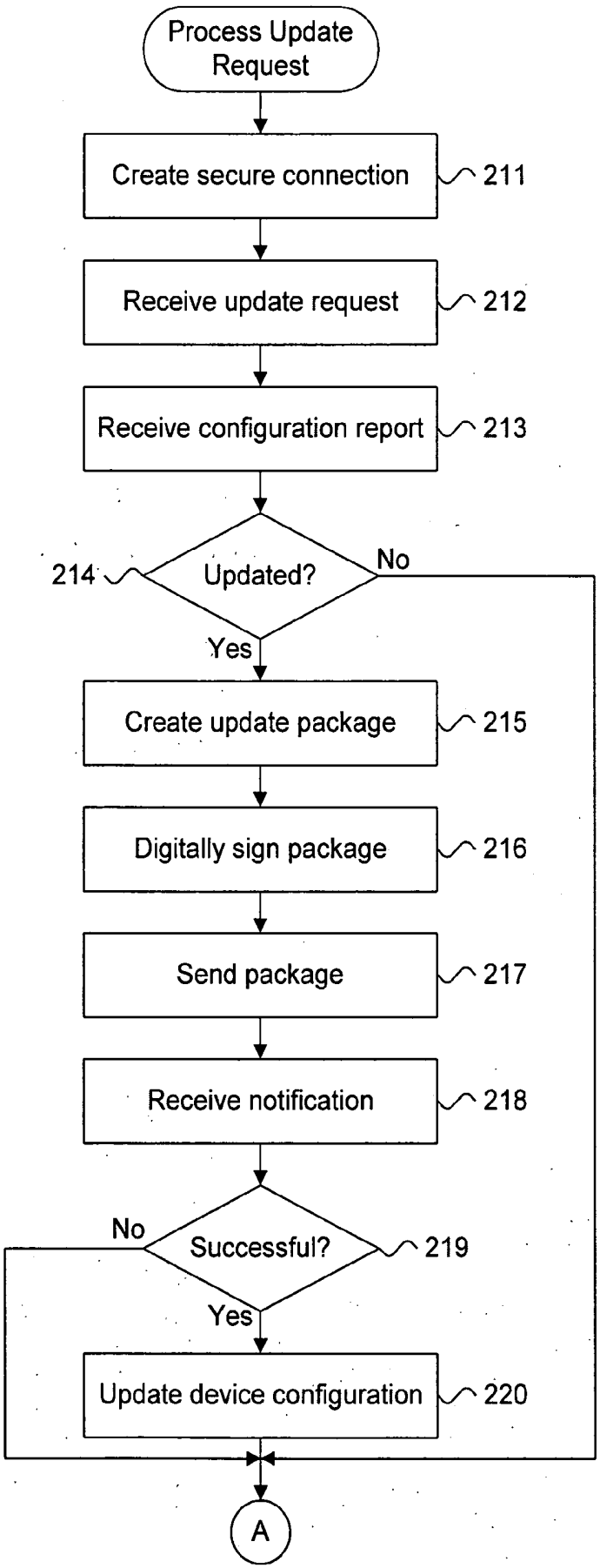

210
Process Update Request
Create secure connection
211
Receive update request
212
Receive configuration report
213
214
Updated?
No
Yes
Create update package
215
Digitally sign package
216
Send package
217
Receive notification
218
No
Successful?
219
Yes
Update device configuration
220
A

Fig. 10 (Cont.).

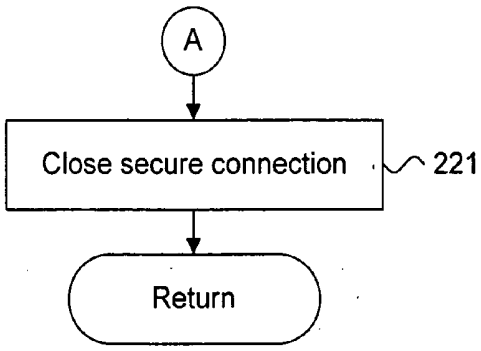


Fig. 11.

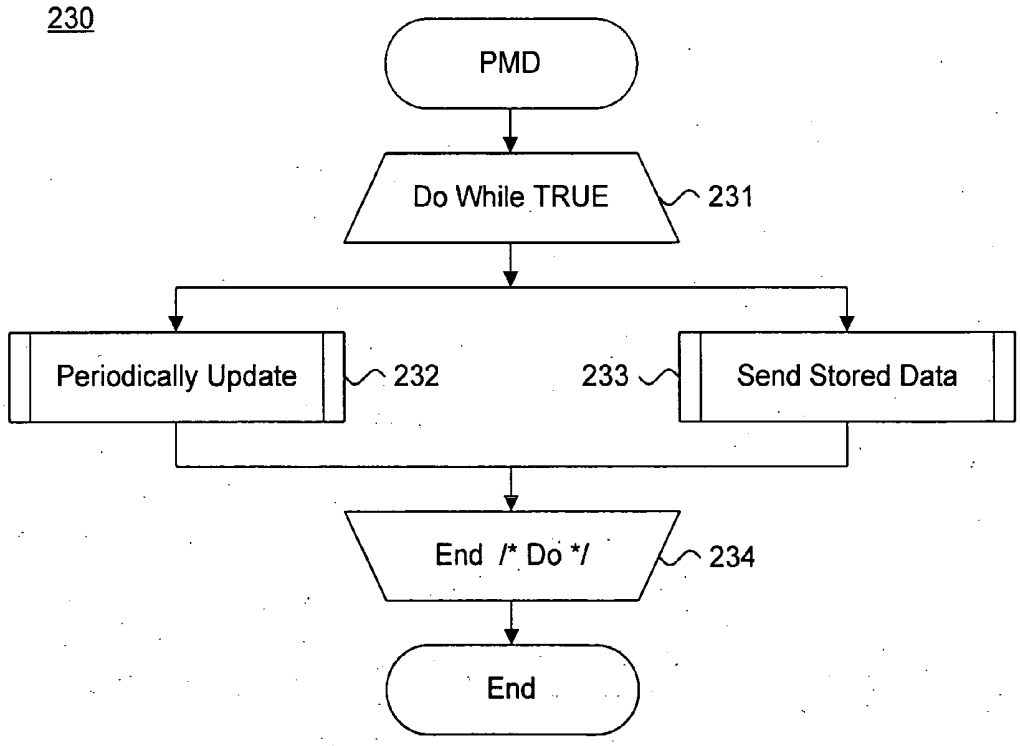


Fig. 12.

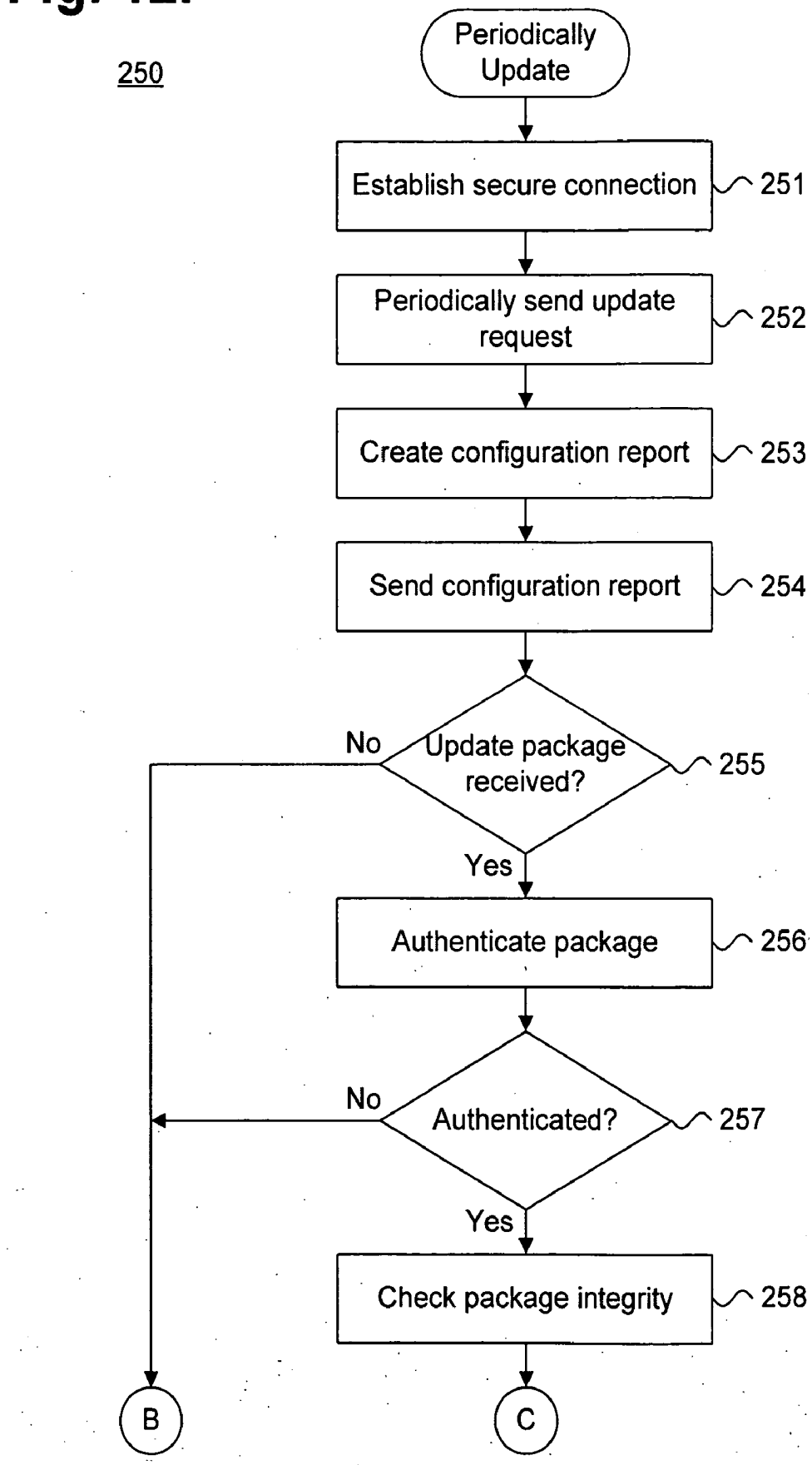

250
Periodically Update
Establish secure connection
251
Periodically send update request
252
Create configuration report
253
Send configuration report
254
Update package received?
255
No
Yes
Authenticate package
256
Authenticated?
257
No
Yes
Check package integrity
258
B
C

Fig. 12 (Cont.).

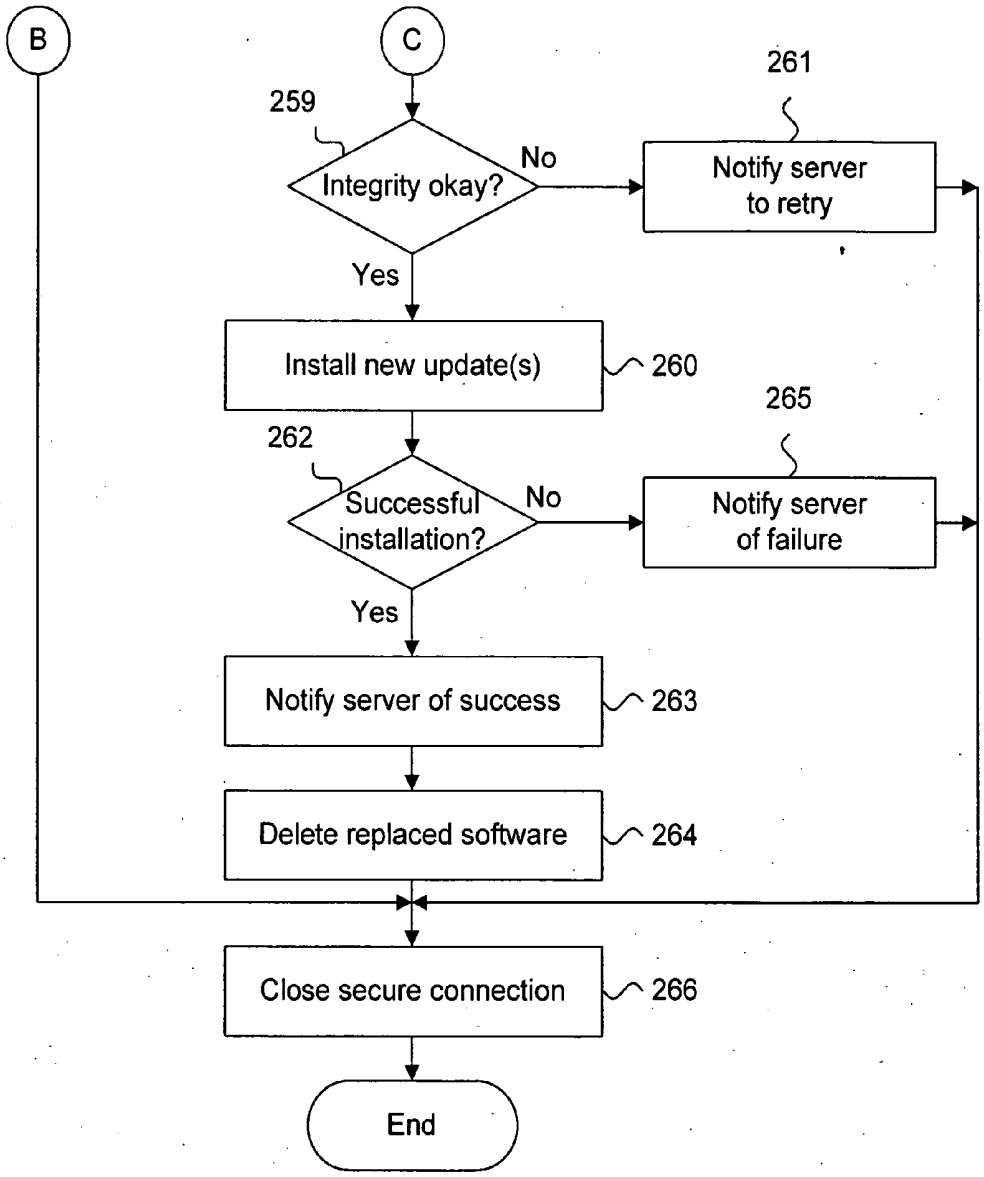
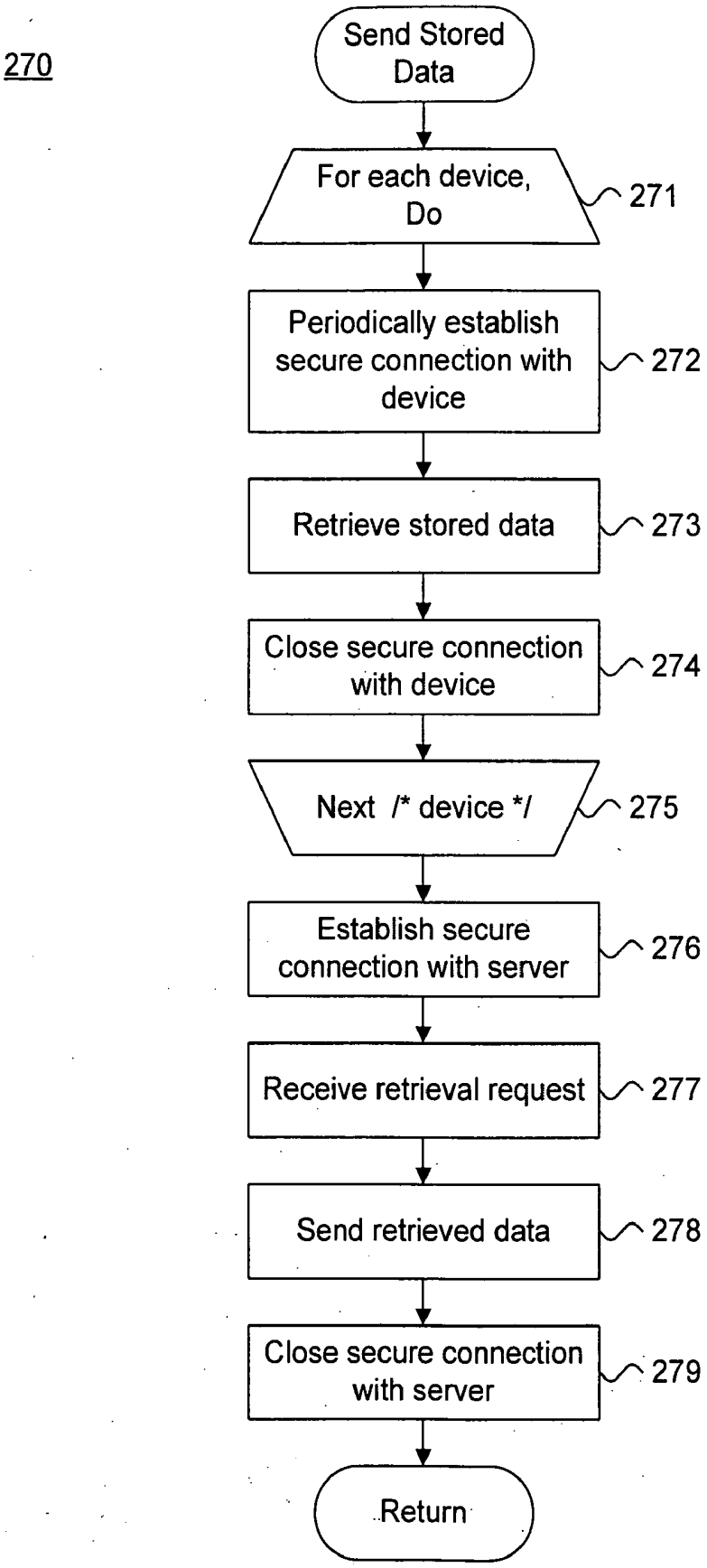

B
C
259
Integrity okay?
No
261
Notify server to retry
Yes
Install new update(s)
260
262
Successful installation?
No
265
Notify server of failure
Yes
Notify server of success
263
Delete replaced software
264
Close secure connection
266
End

Fig. 13.


270
Send Stored Data
For each device, Do
271
Periodically establish secure connection with device
272
Retrieve stored data
273
Close secure connection with device
274
Next /* device */
275
Establish secure connection with server
276
Receive retrieval request
277
Send retrieved data
278
Close secure connection with server
279
Return

SYSTEM AND METHOD FOR PROVIDING A SECURE FEATURE SET DISTRIBUTION INFRASTRUCTURE FOR MEDICAL DEVICE MANAGEMENT

FIELD OF THE INVENTION

[0001] The present invention relates in general to medical device management and, specifically, to a system and method for providing a secure feature set distribution infrastructure for medical device management.

BACKGROUND OF THE INVENTION

[0002] Cardiac implantable medical devices (IMDs), such as pacemakers and implantable cardioverter-defibrillators (ICDs), are generally implanted subdermally over the pectoralis major muscle. A set of leads to deliver cardiac therapy and monitor cardiopulmonary physiology is also implanted transvenously under local anesthesia using either the cephalic and subclavian veins. Power for IMDs is provided conventionally by batteries that have high-energy density, low internal loss, and long shelf life. For example, implanted single-chamber pacemakers use lithium iodine batteries and have an expected implant life of seven to twelve years. Dual-chamber pacemakers use lithium silver vanadium oxide batteries and have an expected implant life of five to ten years.

[0003] Ordinarily, an entire IMD is replaced when the battery life has expired to take advantage of new features and advances in technologies that may have occurred since the time of original implant. Replacement of an IMD requires surgery, which is accompanied by attendant risks of injury, infection, recovery time, and related complications. Surgical risk can be minimized by limiting or eliminating the situations in which a device must be replaced, such as upon the occurrence of a broken or failing lead or problematic IMD.

[0004] Prior to replacement, interim upgrades to the operational characteristics and programming of an IMD can be performed in-clinic by upgrading on-board programming software or firmware using a programmer-type device. These types of updates are limited to a clinical setting and require a physician to be present, which can be problematic if minor yet necessary upgrades need to be performed to a large patient population. Modifications must be precisely matched to the specific model and software or firmware revision level of each IMD. Ensuring correct upgradeability requires extra caution to avoid introducing changes that could harm or render the device inoperable, thereby requiring possible early replacement.

[0005] When available, in-clinic software or firmware upgrades can only be performed under the supervision of a physician. A programmer-type device is used to interrogate the IMD through inductive telemetry. Due to the close proximity of the physician to the patient, authorization is implied and secure exclusive access to the IMD assumed. Software or firmware upgrades are limited to only the device implanted in that patient. Other medical devices, whether implanted or external, must be interrogated and upgraded separately. As a result, managing multiple medical devices requires individually tracking each medical device and the associated operating characteristics for functional upgrades and on-going maintenance on a patient-by-patient basis. This medical device management burden is exacerbated by a large patient population.

[0006] Therefore, there is a need for a medical device management system providing remote, non-surgical upgrades to IMDs. Preferably, such an approach would provide non-clinical and secure, authenticated upgrades to software and firmware used in both implantable and external medical devices on per patient and patient population bases. Such an approach would preferably leverage public infrastructure, such as the Internet, to provide the most economical solution to managing medical devices, while using cryptographic technology to maintain a high level of security and reliability.

SUMMARY OF THE INVENTION

[0007] A system and method includes a secure distribution server maintaining a configuration catalog of unique mappings between a patient management device and one or more associated patient medical devices, including passive and active implantable and external medical devices. Identification of the software and firmware provided on each associated patient medical device is either periodically requested by the patient management device or autonomously reported to the patient management device by each device. In one embodiment, the patient management device requests updates to the software and firmware of the devices and of the patient management device itself from the secure distribution server on a periodic basis and the secure distribution server provides any new or modified sets of features as update packages, which are either already digitally signed by a trusted source or are digitally signed by the secure distribution server for a specific patient management device. In a further embodiment, the secure distribution server periodically provides any new or modified feature sets to the patient management device as such sets become available. The patient management device authenticates the trusted source and checks the integrity of each update package prior to installation. The digital signing by the trusted source is combined with signature verification at each patient management device to ensure the authenticity and integrity of the update package; these processes provide a chain of trust to securely distribute the new or modified feature sets. The patient management device sends a notification back to the secure distribution server upon successful upgrade or installation. In a further embodiment, each device, rather than the patient management device, does performs signature verification of each update package prior to installation to extend the chain of trust to the device itself. Accordingly, both minor and wholesale changes to software and firmware can be distributed to remote devices over one or more networks without the need for an in-clinic patient visit.

[0008] One embodiment provides a system and method for providing a secure feature set distribution infrastructure for medical device management. A unique association is mapped for data download between a medical device and a communications device transiently coupleable to the medical device. A configuration catalog is maintained, including operational characteristics of at least one of the medical device and the communications device. The operational characteristics as maintained in the configuration catalog are periodically checked against a database storing downloadable sets of features and one or more feature sets including

changed operational characteristics are identified for distribution. The one or more feature sets are digitally signed and the one or more feature sets are provided to the communications device over a plurality of networks. The one or more feature sets are authenticated and their integrity is checked over a chain of trust originating with a trusted source and terminating at the communications device.

[0009] Still other embodiments of the present invention will become readily apparent to those skilled in the art from the following detailed description, wherein are described embodiments of the invention by way of illustrating the best mode contemplated for carrying out the invention. As will be realized, the invention is capable of other and different embodiments and its several details are capable of modifications in various obvious respects, all without departing from the spirit and the scope of the present invention. Accordingly, the drawings and detailed description are to be regarded as illustrative in nature and not as restrictive.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] FIG. **1** is a functional block diagram showing a system for providing a secure feature set distribution infrastructure for medical device management in accordance with one embodiment.

[0011] FIG. **2** is a data structure diagram showing, by way of example, a configuration catalog for storing medical device mappings.

[0012] FIG. **3** is a data structure diagram showing, by way of example, an update package for providing an updated feature set.

[0013] FIG. **4** is a block diagram showing the secure distribution server of FIG. **1**.

[0014] FIGS. **5**A-B are routing diagrams showing end-to-end secure package processing by the system of FIG. **1**.

[0015] FIG. **6** is a process flow diagram showing a configuration catalog update dialogue performed by the system of FIG. **1**.

[0016] FIG. **7** is a process flow diagram showing an upload dialogue performed by the system of FIG. **1**.

[0017] FIG. **8** is a flow diagram showing a server method for providing a secure feature set distribution infrastructure for medical device management in accordance with one embodiment.

[0018] FIG. **9** is a flow diagram showing a routine for periodically retrieving data for use in the method of FIG. **7**.

[0019] FIG. **10** is a flow diagram showing a routine for processing an update request for use in the method of FIG. **7**.

[0020] FIG. **11** is a flow diagram showing a method for providing a secure feature set distribution infrastructure for medical device management in accordance with one embodiment.

[0021] FIG. **12** is a flow diagram showing a routine for performing a periodic update for use in the method of FIG. **11**.

[0022] FIG. **13** is a flow diagram showing a routine for sending stored data for use in the method of FIG. **11**.

DETAILED DESCRIPTION

System Overview

[0023] FIG. **1** is a functional block diagram showing a system **10** for providing a secure feature set distribution infrastructure for medical device management in accordance with one embodiment. The system **10** includes a secure distribution server **11** and patient management device **13** that is remotely interconnected via a plurality of networks, including an internetwork **12**, such as the Internet, and intranetworks **15***a*, **15***b*. In one embodiment, each individual network is securely protected at each border by a firewall **16***a*, **16***b*, gateway, or similar security device. Each firewall **16***a*, **16***b* protects an associated network against unauthorized access and intrusion. Other topologies, configurations, and arrangements of networks are possible.

[0024] The secure distribution server **11** is operatively coupled to a storage device **14** and is remotely accessible by the patient management device **13** over the plurality of networks to securely distribute updates or new feature sets, as further described below with reference to FIG. **4**. The patient management device **13** functions primarily as a communications device and executes a set of software modules defined as patient communication application software. In addition, the patient management device **13** can also include medical device functionality. The patient management device **13** includes user interfacing means, including a speaker, microphone, display, interactive user interface, such as a touch screen or keypad, and a secure wireless interface, such as provided by "strong" Bluetooth, wireless fidelity "WiFi" or "WiMax," or other radio frequency interfaces, to allow external and implantable medical devices to be logically interfaced. In one embodiment, the patient management device **13** is implemented as a dedicated hardware device specifically interfacing to external and implantable medical devices. In a further embodiment, the patient management device **13** could be implemented integral to or as an add-on module functionally coupled to a portable computing device, such as a personal digital assistant, cellular telephone, and similar devices.

[0025] Interfaceable external and implantable medical devices include active therapeutic or monitoring devices, such as an implantable medical device **18**, implantable sensor **19**, external medical device **20**, or external sensor **21**, and passive therapeutic or monitoring devices, such as external medical device **22** and external sensor **23**. These therapeutic and monitoring devices can deliver therapy or provide sensor readings that can be processed by the secure distribution server **11** or similar device into quantitative, physiological measures. Implantable medical devices **18** include pacemakers, implantable cardioverter-defibrillators, cardiac resynchronization devices, drug delivery devices, and neurological implants. Implantable sensors **19** include heart or respiratory monitors, and posture, activity, or blood chemistry monitors. Active external medical devices **20** include automated external defibrillators. Active external sensors **21** include Holter monitors. Passive external medical devices **22** include pill dispensers. Finally, passive external sensors **23** include weight scales and blood pressure monitors. Other types of implantable medical devices, implantable sensors, external medical devices, and external sensors, active as well as passive, are possible.

[0026] Operationally, the secure distribution server **11** maintains a configuration catalog of operational character-

istics of the patient management device **13** and the one or more associated medical devices **18-23**. The operational characteristics of the devices are either requested by the patient management device **13** from each device or are periodically reported to the patient management device **13** by each device. The configuration catalog stores a unique association between the patient management device **13** and each medical device for each patient **17**. In one embodiment, the patient management device **13** periodically checks for updates or new feature sets stored as program code by the secure distribution server **11** and then the patient management device securely downloads or "pulls" any modified or new firmware or software, referred to as "updates," as secure packages. Each secure package is either stored on the secure distribution server in digitally signed form, that is, signed by another trusted source, or can be digitally signed by the secure distribution server for a specific patient management device. In a further embodiment, the secure distribution server **11** on-demand or incrementally sends or "pushes" the program code for any modified or new firmware or software to the patient management device **13** as such updates become available or by unilaterally broadcasting the updates to a certain class of devices, such as patient management devices. An on-demand update can be initiated by either the secure distribution server **11** or via an authenticated client on the internetwork **12** or similar device. Upon authenticating and checking the integrity of each update package, the patient management device **13** installs the updated or new feature set on the appropriate medical device and notifies the secure distribution server **11** upon successful completion. In a further embodiment, one or more of the medical devices, rather than the patient management device **13**, authenticate and integrity check each update package prior to installation. Additionally, the secure distribution server **11** or similar device periodically retrieves stored data from the patient management device **13**, which was previously collected from the one or more associated medical devices. The medical device mappings configuration catalog and update packages will now be described.

Medical Device Mappings

[**0027**] FIG. **2** is a data structure diagram showing, by way of example, a configuration catalog **40** for storing medical device mappings. The configuration catalog **40** serves two purposes. First, the configuration catalog **40** maps the unique association between a patient management device **13** and a particular medical device, such as IMD **18**. Second, the configuration catalog **40** records the operational characteristics of both the patient management device **13** and each associated medical device. For instance, an entry can identify the medical device by type **41**, model **42**, serial number **43**, and software revision level **44**. Similarly, the same entry, or a separate linked entry (not shown), can include the patient management device type **45**, model **46**, serial number **47**, and software revision level **48**. Other types of configuration catalog and record structures and arrangements are possible.

[**0028**] The operational characteristics recorded in the configuration catalog **40** can be provided initially by the manufacturer of each device and the patient management device **13**. Subsequently, in one embodiment, the patient management device **13** periodically polls each device to determine current operational characteristics and those operational characteristics, plus operational characteristics of the patient management device **13**, are reported to the secure distribution server **11** to update the configuration catalog **40**. In a further embodiment, the devices periodically report their operational characteristics to the patient management device **13**, which are then reported to the secure distribution server **11** for configuration catalog update. Other forms of configuration catalog updating are possible.

Updated Feature Set

[**0029**] FIG. **3** is a data structure diagram showing, by way of example, an update package **60** for providing an updated feature set. An update package **60** is generated by the secure distribution server **11** to securely distribute modified or new sets of features for a patient management device or one or more associated medical devices. In a further embodiment, an update package **60** can contain a set of "atomic" patches for features that must either be installed as a complete non-divisible set, or not installed at all. In one embodiment, each update package **60** is provided to a patient management device **13** in response to an update request. In a further embodiment, each update package **60** is on-demand or incrementally provided to a patient management device **13** as updated features become available or by unilaterally broadcasting the updated features to a certain class of devices, such as patient management devices. Other forms of secure update package distribution are possible.

[**0030**] Each update package **60** includes a header that identifies the device to which the update code **65** applies, such as device type **61** and model **62**. In addition, the header identifies the pre-updating software revision level **63** and post-updating software revision level **64**, which respectively identify the software revision levels for the update to apply and at which the device will be after the update is installed. In a further embodiment, the pre-updating software revision level **63** can specify a range of pre-updating patch revision levels, or just a single pre-updating patch revision level. The update package **60** is encapsulated within a digitally signed "envelope" (not shown) or package created by the secure distribution server **11**. The update package **60** can either be pre-digitally-signed by a trusted source, such as by the manufacturer, or can be digitally signed by the secure distribution server for a specific patient management device. In one embodiment, update package authentication is provided through a form of asymmetric encryption, such as public/private key-pair based digital signatures, although other types of authentication and encryption are possible.

Secure Distribution Server

[**0031**] FIG. **4** is a block diagram showing the secure distribution server **11** of FIG. **1**. The secure distribution server **11** serves as a focal point for securely distributing modified and new feature sets **77** to patient management devices and associated medical devices. The secure distribution server **11** executes a set of software modules defined as secure distribution server software. The secure distribution server **11** accesses the feature sets **77** through a secure storage device **75**, along with a configuration catalog **76** that maps the unique associations between the patient management device **13** and one of possibly several medical devices for a particular patient **17**.

[**0032**] The secure distribution server **11** includes an update checker and verifier **71** that processes update requests **82** received from remotely-situated patient management

devices **13**. In a further embodiment, the update checker and verifier **71** processes configuration catalog updates **81** received from patient management devices and, in a further embodiment, devices, to update the configuration catalog **76** recording operational characteristics. In a still further embodiment, the update checker and verifier **71** periodically requests configuration catalog updates **81** from the patient management devices and devices. Similarly, update requests **82** can originate directly from a medical device. The update checker and verifier **71** accesses the configuration catalog **76** and identifies any feature sets **77** that are modified or new relative to each stored device configuration. The secure distribution server **11** also includes authentication **72**, which packages any modified or new feature sets **77** into digitally signed packages using a stored asymmetric private key **74** unique to the secure distribution server **11**. Each package is either already digitally signed by a trusted source or can be digitally signed by the secure distribution server using the asymmetric private key **74** and an asymmetric public key for that specific patient management device **13**. The digitally signed feature sets are then sent to the requesting patient management device **13** or, in a further embodiment, a requesting device, as update packages **84**. In a further embodiment, the digitally signed feature sets are on-demand or incrementally sent to the patient management device **13** or, in a still further embodiment, devices, as update packages **84** as modified or new feature sets **77** become available, or by unilaterally broadcasting the updated features to a certain class of devices, such as patient management devices. In addition, the update checker and verifier **71** receives notifications **80** from requesting patient management devices **13** that confirm the successful installation of feature sets **77** and updates the configuration catalog **76**. The operations performed by the update checker and verifier **71** and authentication **72** are further described below with reference to FIG. **10**.

[**0033**] In a further embodiment, the secure distribution server **11** also includes data retrieval, analysis and storage **73**. Periodically, the secure distribution server sends securely a data request **85** to one or more patient management devices **13** to request the upload of data sets **83** of stored data, which the patient management device has collected or from the one or more associated medical devices. The data sets **83** can include physiological quantitative and quality of life qualitative measures for an individual patient collected and processed in conjunction with, by way of example, an implantable medical device, such a pacemaker, ICD, or similar device; an external medical device, such as an electrocardiograph, Holter monitor or similar device; or through conventional medical testing and evaluation. As well, the data sets **83** can be analyzed against one or more medical conditions, such as described in related, commonly-owned U.S. Pat. No. 6,336,903, to Bardy, issued Jan. 8, 2002; U.S. Pat. No. 6,368,284, to Bardy, issued Apr. 9, 2002; U.S. Pat. No. 6,398,728, to Bardy, issued Jun. 2, 2002; U.S. Pat. No. 6,411,840, to Bardy, issued Jun. 25, 2002; and U.S. Pat. No. 6,440,066, to Bardy, issued Aug. 27, 2002, the disclosures of which are incorporated by reference. Finally, the data sets can be stored into a database **78** as retrieved device data **79**. The database **78** need not be directly coupled to the secure distribution server **11** and can be instead remotely accessed through, for instance, a centralized database server (not shown).

[**0034**] In one embodiment, the secure distribution server **11** is a general-purpose server-grade computer, executing a set of software modules defined as secure distribution server software and having components conventionally found in a computer, such as, for example, a central processing unit (CPU), memory, disk storage, network interfaces, display, CD-ROM, keyboard, mouse, and various components for interconnecting these elements.

End-to-End Secure Package Processing

[**0035**] FIGS. **5**A-B are routing diagrams showing end-to-end secure package processing **100**, **120** by the system **10** of FIG. **1**. End-to-end processing involves a secure distribution server and requesting patient management device, which are at the end points of the network infrastructure over which update packages are securely distributed. While in transit, an update package is encapsulated in a "secure digital container" or package that was generated under the digital signature of the source of the update or a secure distribution server.

[**0036**] Referring first to FIG. **5**A, an update source **102** prepares and digitally signs an update package **101**, which is dispatched to a secure distribution server **104** as a signed update **103**. The secure distribution server source **104** authenticates and checks the integrity of the received signed update **103** before storing the signed update **103**. When requested, the secure distribution server **104** dispatches the signed update **103** to a requesting patient management device **105**, which also authenticates and checks the integrity of the received signed update **103** before storing or installing the update **101**. In a further embodiment, the patient management device **105** dispatches the signed update **103** to an IMD **106**, which similarly authenticates and checks the integrity of the received signed update **103** before installing the update **101**.

[**0037**] Referring next to FIG. **5**B, an update source **122** prepares and digitally signs an update package **121**, which is dispatched to a secure distribution server **124** as a signed update **123**. The secure distribution server source **124** authenticates and checks the integrity of the received signed update **123** before storing the signed update **123**. The secure distribution server **124** also adds data **125** to the signed update **123** and digitally signs the entire combined package **126**. When requested, the secure distribution server **124** dispatches the signed combined package **126** to a requesting patient management device **127**, which also authenticates and checks the integrity of the received signed combined package **126** before storing or installing the update **121** and data **125**. In a further embodiment, the patient management device **127** dispatches the signed combined package **126** to an IMD **128**, which similarly authenticates and checks the integrity of the received combined package **126** before installing the update **121** and data **125**. Other forms of end-to-end secure package processing are possible.

Configuration Catalog Update Dialogue

[**0038**] FIG. **6** is a process flow diagram showing a configuration catalog update dialogue **150** performed by the system **10** of FIG. **1**. In one embodiment, the configuration catalog update dialogue is initiated by each patient management device **13**, which periodically connects to one or more associated medical devices (operation **151**) and performing an inventory of operational characteristics (block **152**). The

operational characteristics are then provided to the secure distribution server **11**, which updates the configuration catalog **76** (block **153**). The processing continues again upon the next periodic configuration catalog update (operation **151**). In a further embodiment, each associated medical device periodically connects to a patient management device (operation **151**) and a similar set of operations is followed to inventory operational characteristics and update the configuration catalog.

Upload Dialogue

[**0039**] FIG. **7** is a process flow diagram showing an upload dialogue **160** performed by the system **10** of FIG. **1**. In one embodiment, each patient management device **13** functions as a centralized hub for one or more associated medical devices by periodically connecting to one or more of the devices (operation **161**) and retrieving any stored data (operation **162**) collected by the medical devices. The retrieved data is then sent to the secure distribution server **11** or similar device (operation **163**) for analysis and storage. The process continues upon the next periodic connection by the patient management device **13** (operation **161**).

Server Method Overview

[**0040**] FIG. **8** is a flow diagram showing a server method **170** for providing a secure feature set distribution infrastructure for medical device management in accordance with one embodiment. The purpose of the method is to process update requests at a secure distribution server **11** received from patient management devices **13** on a continuing basis. In a further embodiment, the method **170** also periodically retrieves data stored by the patient management devices **13**.

[**0041**] Initially, a cryptographic key is generated (block **171**). The cryptographic key is generated only once, when the server is initially configured. Depending upon the system, the cryptographic key can be generated by the secure distribution server **11** or installed as part of a manufacturing process; in either case, the cryptographic key is persistently stored by the secure distribution server **11** where the cryptographic key is subsequently used to digitally sign update packages and to establish secure connections with, for example, patient management devices. A secure connection is a communication path over which data can be exchanged without corruption, without observation of the data's content by any third party, and with assurance that the sender and receiver of the data are always known and authenticated.

[**0042**] The initial device configurations of each patient management device **13** and associated medical device are recorded in the configuration catalog **76** (block **172**). Update requests and, in a further embodiment, data retrievals, are processed continuously (blocks **173**-**178**), as follows. In a further embodiment, stored data is periodically retrieved (block **174**) from each patient management device **13**, as further described below with reference to FIG. **9**. Similarly, update requests received from the patient management device **13** are processed (block **175**), as further described below with reference to FIG. **10**. In a still further embodiment, updates of operational characteristics of each patient management device **13** and associated medical devices are recorded in the configuration catalog **76** (block **176**) as provided to the secure distribution server **11**, either in response to a configuration catalog update request or based on a self-generated configuration catalog update from the patient management device or devices. The secure distribution server **11** remains in a standby mode (block **177**) or performs other processing when not actively retrieving data or processing update requests. Processing continues (block **178**) until the secure distribution server **11** terminates operations.

Periodic Data Retrieval

[**0043**] FIG. **9** is a flow diagram showing a routine **190** for periodically retrieving data for use in the method **170** of FIG. **8**. In a further embodiment, the secure distribution server **11** or similar device periodically retrieves data collected and stored by each patient management device **13** and analyzes and stores the retrieved data into a database. This periodic data retrieval method may be initiated by either the server or the patient management device.

[**0044**] The server and the patient management device connect to each other over a network using a secure cryptographic method to authenticate, each to the other (block **191**), to establish a shared cryptographic connection key (block **192**), and to establish a cryptographically protected secure connection (block **193**). The connection establishes a "session" each time a server or patient management device needs to exchange data. A single connection is established, which remains open for the duration of the session. Any data stored by the patient management device **13** is retrieved by the server and the integrity of the data is checked to ensure that no modifications occurred while the data was in transit (block **194**). The data is stored into the database (block **195**) and the server instructs the patient management device **13** to delete the data (block **196**). The secure connection is then closed (block **197**) and the retrieved data can be further processed by the secure distribution server **11** (block **198**), as further described above with reference to FIG. **8**.

Update Request Processing

[**0045**] FIG. **10** is a flow diagram showing a routine **210** for processing an update request for use in the method **170** (block **175**) of FIG. **8**. The purpose of this routine is to process update requests received from each patient management device **13**.

[**0046**] A secure connection with the requesting patient management device **13** is created (block **211**) and an update request **82** is received (block **212**). The connection establishes a "session" each time a server or patient management device needs to exchange data. A single connection is established, which remains open for the duration of the session. In a further embodiment, a non-secure connection could be used if data confidentiality were not a concern. A configuration report is received from the requesting patient management device **13** (block **213**) and the configuration catalog is checked for updates (block **214**). If the program code for any of the software or firmware has been updated (block **214**), an update package is created (block **215**) and digitally signed for the requesting patient management device **13** (block **216**) using the digital signature **74** for the secure distribution server **11** (shown in FIG. **4**). In a further embodiment, the update package is already digitally signed and the secure distribution server **11** only retrieves the update package from storage **14**. In a still further embodiment, the secure distribution server **11** on-demand or incrementally provides any modified or new firmware or software to the patient management device **13** as such updates

become available, or by unilaterally broadcasting the updates to certain class of devices, such as patient management devices. The digitally signed package is sent to the requesting patient management device **13** or, in a further embodiment, one or more of the medical devices (block **217**) and the secure distribution server **11** awaits receipt of notification of successful install (block **218**). If successful (block **219**), the device configuration in the configuration catalog **76** is updated (block **220**). The secure connection is then closed (block **221**).

[**0047**] In the absence of failure conditions affecting the connection between the patient management device **13** and the secure distribution server **11**, the new or modified feature sets and acknowledgement notifications are communicated over a connection that is assumed to be reliable. However, error conditions, such as corrupted or lost data, can be handled by introducing error detecting and correcting functionality into the internetwork **12**, either in addition to or in lieu of the error detection and correction provided by the lower layers of the network protocols implemented by the internetwork **12**. For example, in one embodiment, the internetwork **12** is based on the Transmission Control Protocol/Internet Protocol (TCP/IP) network communication specification, which guarantees reliable message transport. Other network implementations are possible. For instance, the User Datagram Protocol (UDP) could be employed instead of TCP, at the cost of guaranteed data delivery, relying instead on upper protocol layers to provide the necessary error detection and correction. Similarly, other network topologies and arrangements are possible.

Method Overview

[**0048**] FIG. **11** is a flow diagram showing a method **230** for providing a secure feature set distribution infrastructure for medical device management in accordance with one embodiment. The purpose of the patient management device method is to update the program code for the software and firmware installed on each associated medical device, as well as on the patient management device itself. In a further embodiment, each patient management device **13** collects and stores data from each of the associated medical devices for subsequent retrieval by the secure distribution server **11** or similar device.

[**0049**] The program code for the software and firmware is periodically updated and, in a further embodiment, stored data sent, in a continuous processing loop (blocks **231-234**), as follows. The program code for the firmware and software is periodically updated (block **232**), as further described below with reference to FIG. **12**. In a further embodiment, data collected and stored from each associated medical device is sent to the secure distribution server **11** or similar device (block **233**), as further described below with reference to FIG. **13**.

Periodic Update

[**0050**] FIG. **12** is a flow diagram showing a routine **250** for performing a periodic update for use in the method **230** of FIG. **11**. The purpose of this routine is to periodically request and install an update of the program code for the firmware and software in each associated medical device, as well as in a requesting patient management device **13** itself.

[**0051**] A secure connection with the secure distribution server **11** is established (block **251**). The connection establishes a "session" each time a server or patient management device needs to exchange data. A single connection is established, which remains open for the duration of the session. An update request **82** is periodically sent to the secure distribution server **11** (block **252**). The configuration report for each of the associated medical devices and the requesting patient management device **13** is created (block **253**) and sent to the secure distribution server **11** over the secure connection (block **254**). If an update package **84** is received (block **255**), the package is authenticated (block **256**). Otherwise, if no update package is received (block **255**), the secure connection with the secure distribution server **11** is closed (block **266**). If successfully authenticated (block **257**), the integrity of the package is checked (block **258**). Otherwise, if the authentication fails (block **257**), the secure connection with the secure distribution server **11** is closed (block **266**). If the integrity is sound (block **259**), each update included in the package is installed (block **260**). Otherwise, if the integrity is corrupt (block **259**), the server is notified to retry the update request (block **261**). If successful installation (block **262**), the secure distribution server **11** is notified (block **263**) and the replaced program code for the software or firmware is deleted (block **264**). Otherwise, if installation is not successful (block **262**), the server is notified of the failure (block **265**). Finally, the secure connection with the secure distribution server **11** is closed (block **266**). In a further embodiment, one or more of the medical devices, rather than a patient management device **13**, establishes a secure connection with the secure distribution server **11** and receives, authenticates, and checks the integrity of, and installs the update packages **84**. In a still further embodiment, packages **84** can be unilaterally broadcast from the secure distribution server **11** to update a certain class of devices, such as patient management devices, and each such update is installed automatically or, at the next appropriate opportunity.

[**0052**] In a still further embodiment, the patient management device can receive and store updates for classes of devices with which the patient management device communicates for subsequent transfer to the devices and the devices will then apply the updates.

Stored Data Sending

[**0053**] FIG. **13** is a flow diagram showing a routine **270** for sending stored data for use in the method **230** of FIG. **11**. In a further embodiment, the purpose of this routine is to collect and temporarily store data from each associated medical device for subsequent retrieval by the secure distribution server **11** or similar device.

[**0054**] Initially, each device is polled in a processing loop (blocks **271-275**), as follows. A secure connection is periodically established with each medical device (block **272**). Any data stored since the last secure connection is retrieved (block **273**) and the secure connection is closed (block **274**). Periodically, the secure distribution server **11** or similar device establishes a secure connection with the patient management device **13** (block **276**). The connection establishes a "session" each time a server or patient management device needs to exchange data. A single connection is established, which remains open for the duration of the session. The patient management device **13** receives a retrieval request from the secure distribution server **11** or similar device (block **276**) and the retrieved data is sent

(block **278**). Finally, the secure connection with the secure distribution server **11** or similar device is closed (block **279**).

[**0055**] In a further embodiment, one or more of the devices initiates an upload of temporarily stored data to the patient management device. **13**, secure distribution server **11**, or similar device. The device can initiate the upload according to a predefined schedule or could employ polling by the receiving system. Other forms of data upload and exchange are possible, including combinations of push, pull, and scheduled data exchange.

[**0056**] While the invention has been particularly shown and described as referenced to the embodiments thereof, those skilled in the art will understand that the foregoing and other changes in form and detail may be made therein without departing from the spirit and scope of the invention.

What is claimed is:

1. A system for providing a secure feature set distribution infrastructure for medical device management, comprising:

a unique association map for data download between a medical device and a communications device transiently coupleable to the medical device;

a configuration catalog comprising operational characteristics of at least one of the medical device and the communications device;

an update checker to periodically check the operational characteristics as maintained in the configuration catalog against a database storing downloadable sets of features and to identify one or more feature sets comprising changed operational characteristics for distribution, wherein the one or more feature sets are digitally signed and the one or more feature sets are provided to the communications device over a plurality of networks; and

an authenticator to authenticate and check the integrity of the one or more feature sets over a chain of trust originating with a trusted source and terminating at the communications device.

2. A system according to claim 1, wherein the trusted source is a secure distribution server.

3. A system according to claim 1, wherein the one or more feature sets are sent to the communications device in response to a download request.

4. A system according to claim 1, wherein the one or more feature sets are sent on-demand or incrementally or are unilaterally broadcast from a secure distribution server to the communications device.

5. A system according to claim 1, further comprising:

an installer to update the at least one of the medical device and the communications device with the one or more feature sets, and to send a notification to the secure distribution server following successful updating.

6. A system according to claim 1, further comprising:

a collector to regularly collect physiological measures from at least one of the medical device into the communications device, and to provide the collected physiological measures in response to an upload request periodically received.

7. A system according to claim 1, further comprising:

a further map to map associations for data upload between at least one further medical device and the communications device transiently coupleable to the at least one further medical device.

8. A system according to claim 1, further comprising:

a further map to map unique associations for data download between a plurality of medical devices and the communications device transiently coupleable to each such medical device.

9. A system according to claim 1, wherein the one or more feature sets comprises program code comprising at least one of a firmware and a software update.

10. A system according to claim 1, wherein the medical device comprises at least one of an implantable medical device and an external medical device.

11. A system according to claim 1, wherein the medical device comprises at least one of a pacemaker, implantable cardioverter-defibrillator, cardiac resynchronization device, neurological implant, heart monitor, respiratory monitor, automated external defibrillator, Holter monitor, pill dispenser, weight scale, and blood pressure monitor.

12. A system according to claim 1, wherein the medical device comprises at least one of a patient communications device, repeater, programmer, and programmer/recorder.

13. A method for providing a secure feature set distribution infrastructure for medical device management, comprising:

mapping a unique association for data download between a medical device and a communications device transiently coupleable to the medical device;

maintaining a configuration catalog comprising operational characteristics of at least one of the medical device and the communications device;

periodically checking the operational characteristics as maintained in the configuration catalog against a database storing downloadable sets of features and identifying one or more feature sets comprising changed operational characteristics for distribution;

digitally signing the one or more feature sets and providing the one or more feature sets to the communications device over a plurality of networks; and

authenticating and checking the integrity of the one or more feature sets over a chain of trust originating with a trusted source and terminating at the communications device.

14. A method according to claim 13, wherein the trusted source is a secure distribution server.

15. A method according to claim 13, further comprising:

sending the one or more feature sets to the communications device in response to a download request.

16. A method according to claim 13, further comprising:

sending the one or more feature sets to the communications device in response to a download request.

17. A method according to claim 13, further comprising:

on-demand or incrementally sending or unilaterally broadcasting the one or more feature sets from a secure distribution server to the communications device.

18. A method according to claim 13, further comprising:

updating the at least one of the medical device and the communications device with the one or more feature sets; and

sending a notification from a secure distribution server following successful updating.

19. A method according to claim 13, further comprising:

regularly collecting physiological measures from at least one of the medical device into the communications device; and

providing the collected physiological measures in response to an upload request periodically received.

20. A method according to claim 13, further comprising:

mapping associations for data upload between at least one further medical device and the communications device transiently coupleable to the at least one further medical device.

21. A method according to claim 13, further comprising:

mapping unique associations for data download between a plurality of medical devices and the communications device transiently coupleable to each such medical device.

22. A method according to claim 13, wherein the one or more feature sets comprises program code comprising at least one of a firmware and a software update.

23. A method according to claim 13, wherein the medical device comprises at least one of an implantable medical device and an external medical device.

24. A method according to claim 13, wherein the medical device comprises at least one of a pacemaker, implantable cardioverter-defibrillator, cardiac resynchronization device, neurological implant, heart monitor, respiratory monitor, automated external defibrillator, Holter monitor, pill dispenser, weight scale, and blood pressure monitor.

25. A method according to claim 13, wherein the medical device comprises at least one of a patient communications device, repeater, programmer, and programmer/recorder.

26. A computer-readable storage medium holding code for performing the method according to claim 13.

27. An apparatus for providing a secure feature set distribution infrastructure for medical device management, comprising:

means for mapping a unique association for data download between a medical device and a communications device transiently coupleable to the medical device;

means for maintaining a configuration catalog comprising operational characteristics of at least one of the medical device and the communications device;

means for periodically checking the operational characteristics as maintained in the configuration catalog against a database storing downloadable sets of features and means for identifying one or more feature sets comprising changed operational characteristics for distribution;

means for digitally signing the one or more feature sets and means for providing the one or more feature sets to the communications device over a plurality of networks; and

means for authenticating and means for checking the integrity of the one or more feature sets over a chain of trust originating with a trusted source and terminating at the communications device.

* * * * *

专利名称(译)	用于为医疗设备管理提供安全功能集分发基础设施的系统和方法		
公开(公告)号	US20070136098A1	公开(公告)日	2007-06-14
申请号	US11/299980	申请日	2005-12-12
[标]申请(专利权)人(译)	斯迈思ALAN ^ h SIMMS HOWARDÐ HOYME KENNETH P JELATIS GEORGEÐ		
申请(专利权)人(译)	斯迈思ALAN ^ h SIMMS HOWARDÐ HOYME KENNETH P JELATIS GEORGEÐ		
当前申请(专利权)人(译)	斯迈思ALAN ^ h SIMMS HOWARDÐ HOYME KENNETH P JELATIS GEORGEÐ		
[标]发明人	SMYTHE ALAN H SIMMS HOWARD D HOYME KENNETH P JELATIS GEORGE D		
发明人	SMYTHE, ALAN H. SIMMS, HOWARD D. HOYME, KENNETH P. JELATIS, GEORGE D.		
IPC分类号	A61B5/00 G06F19/00 G06F12/14 G06F15/173		
CPC分类号	A61N1/08 A61N1/37252 A61N1/37264 G06F19/3412 G06Q50/24 H04L63/123 H04L63/126 H04L67/34 H04L67/12 A61N1/37254 G16H40/40 G16H40/67		
外部链接	Espacenet USPTO		

摘要(译)

提出了一种用于为医疗设备管理提供安全特征集分发基础设施的系统和方法。映射用于医疗设备和可临时耦合到医疗设备的通信设备之间的数据下载的唯一关联。维护配置目录，包括医疗设备和通信设备中的至少一个的操作特性。根据存储可下载特征集的数据库定期检查配置目录中维护的操作特性，并识别包括改变的操作特性的一个或多个特征集以进行分发。对一个或多个特征集进行数字签名，并且通过多个网络将一个或多个特征集提供给通信设备。对一个或多个特征集进行认证，并通过源自可信源并终止于通信设备的信任链来检查它们的完整性。