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

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2539998 C 2012/10/09

(11)(21) 2 539 998

(12) BREVET CANADIEN
CANADIAN PATENT

(13) C

(22) Date de dépôt/Filing Date: 2006/03/17

(41) Mise à la disp. pub./Open to Public Insp.: 2006/10/04

(45) Date de délivrance/Issue Date: 2012/10/09

(30) Priorité/Priority: 2005/04/04 (EP05102623.5)

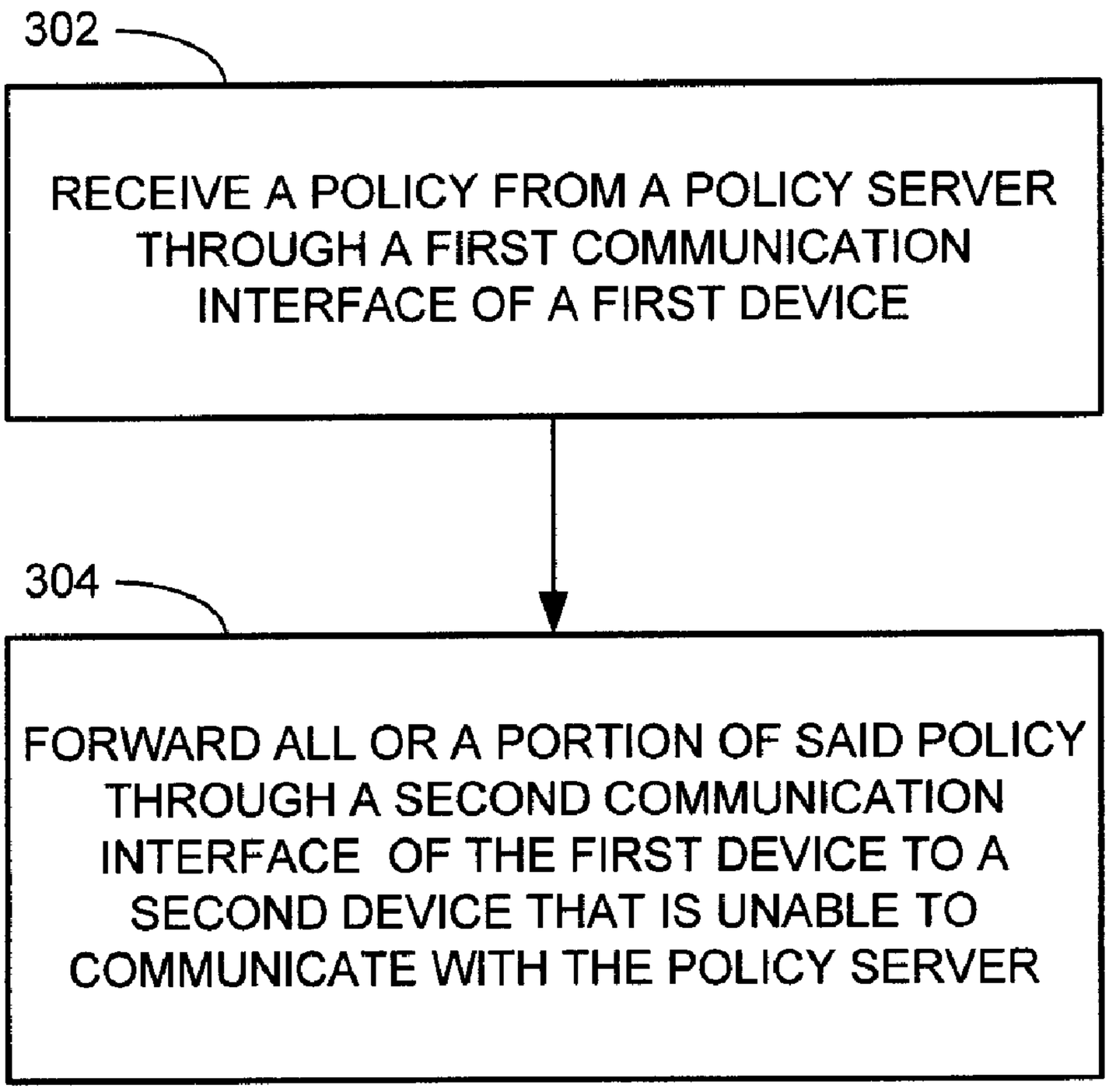
(51) Cl.Int./Int.Cl. *H04L 29/02* (2006.01),
H04L 29/10 (2006.01)

(72) Inventeurs/Inventors:
BROWN, MICHAEL K., CA;
ADAMS, NEIL, CA;
LITTLE, HERBERT, CA

(73) Propriétaire/Owner:
RESEARCH IN MOTION LIMITED, CA

(74) Agent: INTEGRAL IP

(54) Titre : SERVEUR PROXY DE PROGRAMME D'ACTION DE SECURITE
(54) Title: POLICY PROXY



(57) Abrégé/Abstract:
A first device is able to communicate with a policy server and with a second device, but the second device is unable to communicate with the policy server. The first device makes, on its own initiative, a request of the policy server. The request is for the policy server to send to the first device a policy for the second device. The first device then sends all or a portion of the policy to the second device.

ABSTRACT

A first device is able to communicate with a policy server and with a second device, but the second device is unable to communicate with the policy server. The first device makes, on its own initiative, a request of the policy server. The request is for the policy server to send to the first device a policy for the second device. The first device then sends all or a portion of the policy to the second device.

RIM017-03CA

POLICY PROXY

TECHNICAL FIELD

[0001] The invention is related to the technical field of delivery of IT policies from a policy server to devices.

BACKGROUND

[0002] In an organization, an Information Technology (IT) administrator may create IT policies to control the electronic devices in the organization, such as computers, laptops, cellphone, personal digital assistants, printers, and the like. A policy server may store the various IT policies, and may push the relevant IT policy directly to the devices in the organization. Alternatively, the devices may contact the policy server directly to obtain their IT policy.

[0003] The organization may include electronic devices that are unable to connect to the policy server. The IT administrator may manually configure each such electronic device according to the established IT policy. However, this is time-consuming and may lead to errors if the manual configuration does not match the intended policy. Moreover, some electronic devices may not include a user interface that is suitable for enabling configuration according to an IT policy.

[0004] The IT administrator may also develop IT policies for electronic devices that do not belong to the organization but that communicate with a device that does belong to the organization, or have installed thereon software for use with devices that belong to the organization. Since these devices do not belong to the organization, they may be unable to connect to the policy server and the IT administrator may not have any physical access to them.

SUMMARY

[0005] A first device is able to communicate with a policy server and with a second device, but the second device is unable to communicate with the policy server. The first device makes, on its own initiative, a request of the policy server. The request is for the policy

server to send to the first device a policy for the second device. The first device then sends all or a portion of the policy to the second device.

[0006] The communication between the first device and the second device may be over a wireless communication link, for example, a Bluetooth® link. The communication between the first device and the policy server may be over a communication link at least a portion of which is wireless, for example, a cellular telephony network and/or a wireless local area network.

[0007] The second device may be, for example, a smart card reader. The policy may include any or a combination of the following: under what circumstances confidential information stored at the smart card reader is deleted; with which devices other than the first device the smart card reader is allowed to communicate; the number of incorrect smart card login attempts before the smart card reader is locked; and which algorithms smart card reader is allowed to use to protect a communication link with the first device.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] Embodiments of the invention are illustrated by way of example and not limitation in the figures of the accompanying drawings, in which like reference numerals indicate corresponding, analogous or similar elements, and in which:

[0009] Figure 1 is a schematic diagram of an exemplary system, according to some embodiments of the invention;

[0010] Figure 2 is a block diagram of some component of the exemplary system of figure 1, according to some embodiments of the invention; and

[0011] Figure 3 a flowchart of an exemplary method, according to some embodiments of the invention.

[0012] It will be appreciated that for simplicity and clarity of illustration, elements shown in the figures have not necessarily been drawn to scale. For example, the dimensions of some of the elements may be exaggerated relative to other elements for clarity.

DETAILED DESCRIPTION

[0013] In the following detailed description, numerous specific details are set forth in order to provide a thorough understanding of embodiments of the invention. However it will be understood by those of ordinary skill in the art that the embodiments of the invention may be practiced without these specific details. In other instances, well-known methods, procedures, components and circuits have not been described in detail so as not to obscure the embodiments of the invention.

[0014] Figure 1 is a schematic diagram of an exemplary system, according to some embodiments of the invention. A system 100 includes a device 102 and a policy server 110. An IT administrator may store one or more policies on policy server 110. One or more of the policies stored on policy server 110 may apply to device 102, and policy server 110 may push the one or more policies that apply to device 102 over a communication link 120. Device 102 may contact policy server 110 over communication link 120 to request the one or more policies that apply to device 102.

[0015] System 100 may also include other devices for which the IT administrator has stored policies on policy server 110. For example, these other devices may include a smart card reader 104, a personal computer 106, and a printer 108, which may be able to communicate with device 102 over communication links 114, 116 and 118, respectively. A smart card 103 is shown inserted into smart card reader 104. Smart card reader 104 and printer 108 may be considered peripherals of device 102, and one or more software applications for use with device 102 may be installed on personal computer 106.

[0016] Device 102 may be a mobile device, and communication link 120 may include a segment that is a wireless communication link. For example, communication link 120 may include a cellular telephony link. A non-exhaustive list of examples of cellular telephony standards for the cellular telephony link includes Direct Sequence – Code Division Multiple Access (DS-CDMA), Global System for Mobile Communications (GSM), North American Digital Cellular (NADC), Time Division Multiple Access (TDMA), Extended-TDMA (E-TDMA), wideband CDMA (WCDMA), General Packet Radio Service (GPRS), Enhanced Data for GSM Evolution (EDGE), 3.5G and 4G. In another example, communication link 120 may include a wireless local area network link. A non-exhaustive list of examples of wireless

local area network standards for the wireless local area network link includes the Institute of Electrical and Electronic Engineers (IEEE) for Wireless LAN MAC and Physical layer (PHY) 802.11 a, b, g and n specifications or future related standards, the Bluetooth® standard, the Zigbee™ standard and the like.

[0017] Smart cards are personalized security devices, defined by the ISO7816 standard and its derivatives, as published by the International Organization for Standardization. A smart card may have a form factor of a credit card and may include a semiconductor device. The semiconductor device may include a memory that can be programmed with a secret key and with an authentication certificate, and may include a decryption engine, e.g., a processor and/or dedicated decryption logic. A smart card may include a connector for powering the semiconductor device and performing serial communication with an external device. Alternatively, smart card functionality may be embedded in a device having a different form factor and different communication protocol, for example a Universal Serial Bus (USB) device.

[0018] The person whose security information is stored on smart card 103 may use smart card reader 104 for identification and to digitally sign and/or decrypt messages sent by device 102. Smart card reader 104 may communicate with device 102 over a wireless communication link 114, for example, a Bluetooth® communication link.

[0019] A non-exhaustive list of examples of what an IT policy for smart card reader 104 may include is a) under what circumstances confidential information stored at smart card reader 104 is deleted, b) with which devices smart card reader 104 is allowed to communicate, c) the number of incorrect smart card login attempts before smart card reader 104 is locked, and d) which algorithms smart card reader 104 is allowed to use to protect wireless communication link 114. However, smart card reader 104 may lack a user interface that is suitable for configuring this policy in smart card reader 104. Also, smart card reader 104 may be unable to communicate with policy server 110. Policy server 110 may communicate a policy for smart card reader 104 to device 102, and device 102 may communicate the policy to smart card reader 104.

[0020] Printer 108 may be a local printer that communicates with device 102 over wireless communication link 118, for example, a Bluetooth® communication link. A non-exhaustive list of examples of what an IT policy for printer 108 may include is a)font or

template information on how to print out forms of the organization, b) printer resolution (e.g., dots per inch), and c) which devices printer 108 is allowed to connect to. Printer 108 may be unable to communicate with policy server 110. Policy server 110 may communicate a policy for printer 108 to device 102, and device 102 may communicate the policy to printer 108.

[0021] Personal computer 106 may be a home computer of a person who belongs to the organization, and may have a software application installed thereon for use with device 102. An IT policy for personal computer 106 may, for example, affect how the software application operates. Policy server 110 may communicate a policy for personal computer 106 to device 102, and device 102 may communicate the policy to personal computer 106.

[0022] In general, policy server 110 may communicate to device 102 a policy for another device that is able to communicate with device 102 and unable to communicate with policy server 110, and device 102 may communicate the policy to the other device. Device 102 may contact policy server 110 over communication link 120 to request one or more policies for the other device. Device 102 may collect information regarding which other devices it is communicating with and may report that information to policy server 110. Device 102 may also send a confirmation back to policy server 110 once a policy received at device 102 and communicated to another device is applied at the other device.

[0023] Figure 2 is an exemplary block diagram of policy server 110, device 102 and device 104, according to some embodiments of the invention.

[0024] Device 102 may include a communication interface 202 through which device 102 is able to receive a policy from policy server 110. Device 102 may also include a communication interface 204 through which device 102 is able to transmit all or a portion of the policy to device 104. Communication interface 202 may be compatible, for example, with a wireless local area network standard or with a cellular telephony standard. Communication interface 204 may be compatible, for example, with the Bluetooth® standard. Communication interface 202 and communication interface 204 may be a single interface.

[0025] Device 102 may also include a processor 206 coupled to communication interface 202 and to communication interface 204. Device 102 may also include a memory 208, coupled to processor 206. Memory 208 may store executable code 209 to be executed by

processor 206. Memory 208 is able to store one or more policies received from policy server 110.

[0026] Policy server 110 may include a communication interface 212, a processor 216 coupled to communication interface 212, and a memory 218 coupled to processor 216. Memory 218 is able to store IT policies.

[0027] Device 104 may include a communication interface 224, a processor 226 coupled to communication interface 224, and a memory 228 coupled to processor 226. Memory 228 is able to store one or more policies received from device 102. Communication interface 224 may be compatible with the same standard as communication interface 204.

[0028] Figure 3 is a flowchart of an exemplary method to be implemented by device 102, according to some embodiments of the invention. Executable code 209, when executed by processor 210, may cause device 102 to implement the method of figure 3.

[0029] At 302, device 102 receives a policy from policy server 110 through communication interface 202 over communication link 120. At 304, device 102 transmits all or a portion of the policy through communication interface 204 to another device that is unable to communicate with policy server 110.

[0030] A non-exhaustive list of examples for device 102 includes a cellular phone, a personal digital assistant (PDA), an electronic mail (Email) client, a gaming device, a laptop computer, a notebook computer, a desktop computer, a server computer, and any other suitable apparatus.

[0031] A non-exhaustive list of examples for processors 206, 216 and 226 includes a central processing unit (CPU), a digital signal processor (DSP), a reduced instruction set computer (RISC), a complex instruction set computer (CISC) and the like.

[0032] Memories 208, 218 and 228 may be fixed in or removable from device 102, policy server 110 and device 104, respectively. A non-exhaustive list of examples for memories 208, 218 and 228 includes any combination of the following:

a) semiconductor devices such as registers, latches, read only memory (ROM), mask ROM, electrically erasable programmable read only memory devices (EEPROM), flash memory devices, non-volatile random access memory devices

(NVRAM), synchronous dynamic random access memory (SDRAM) devices, RAMBUS dynamic random access memory (RDRAM) devices, double data rate (DDR) memory devices, static random access memory (SRAM), universal serial bus (USB) removable memory, and the like;

b) optical devices, such as compact disk read only memory (CD ROM), and the like; and

c) magnetic devices, such as a hard disk, a floppy disk, a magnetic tape, and the like.

[0033] Processors 206, 216 and 226, and memories 208, 218 and 228 are functional blocks and may be implemented in any physical way in device 102, policy server 110 and device 104, respectively. For example, processor 206 and memory 208 may each be implemented in a separate integrated circuit, and optionally in additional discrete components. Alternatively, some of the functional blocks may be grouped in one integrated circuit. Furthermore, the functional blocks may be parts of application specific integrated circuits (ASIC), field programmable gate arrays (FPGA) or application specific standard products (ASSP).

[0034] While certain features of the invention have been illustrated and described herein, many modifications, substitutions, changes, and equivalents will now occur to those of ordinary skill in the art. It is, therefore, to be understood that the appended claims are intended to cover all such modifications and changes as fall within the scope of the invention.

What is claimed is:

1. A system comprising:

a policy server;

a first device able to communicate with said policy server;

one or more other devices able to communicate with said first device and unable to communicate with said policy server,

wherein said first device is to collect information regarding those of said other devices with which said first device is communicating, to report said information to said policy server, to contact said policy server to request a policy for one of said other devices, to receive from said policy server a policy for said one of said other devices, and to send all or a portion of said policy to said one of said other devices.

2. The system of claim 1, wherein said one of said other devices is a smart card reader or a printer.

3. The system of claim 1, wherein said one of said other devices has installed thereon a software application for use with said first device, and said policy affects how said software application operates.

4. The system of claim 1, wherein said one of said other devices is a smart card reader and said policy defines under what circumstances confidential information stored at said smart card reader is deleted.

5. The system of claim 1, wherein said one of said other devices is a smart card reader and said policy defines with which devices other than said first device said smart card reader is allowed to communicate.

6. The system of claim 1, wherein said one of said other devices is a smart card reader and said policy defines the number of incorrect smart card login attempts following which said smart card reader is to be locked.

7. The system of claim 1, wherein said one of said other devices is a smart card reader and said policy defines which algorithms said smart card reader is allowed to use to protect a communication link with said first device.

8. The system of any one of claims 1 to 7, wherein said first device is a mobile device and said one of said other devices is able to communicate with said mobile device over a wireless communication link.

9. The system of claim 8, wherein said wireless communication link is a Bluetooth® communication link.

10. The system of any one of claims 1 to 9, wherein said first device is a mobile device and said first device is able to communicate with said policy server over a communication link at least a segment of which is a wireless communication link.

11. The system of claim 10, wherein said wireless communication link is a cellular telephony link or a wireless local area network link.

12. A system comprising:

a policy server;

a first device able to communicate with said policy server;

a second device able to communicate with said first device and unable to communicate with said policy server,

wherein said policy server is to push to said first device a policy for said second device, and said first device is to push said policy to said second device.

13. The system of claim 12, wherein said first device is a mobile device and said second device is able to communicate with said mobile device over a wireless communication link.

14. The system of claim 13, wherein said second device is a smart card reader.

15. The system of claim 14, wherein said policy defines under what circumstances confidential information stored at said smart card reader is deleted.

16. The system of claim 14, wherein said policy defines with which devices other than said first device said smart card reader is allowed to communicate.

17. The system of claim 14, wherein said policy defines the number of incorrect smart card login attempts after which said smart card reader is locked.

18. The system of claim 14, wherein said policy defines which algorithms said smart card reader is allowed to use to protect a communication link with said first device.

19. The system of claim 13, wherein said second device is a printer.

20. The system of claim 19, wherein said policy defines font information for said printer.

21. The system of claim 19, wherein said policy defines template information for said printer.

22. The system of claim 19, wherein said policy defines a printer resolution for said printer.

23. The system of claim 19, wherein said policy defines with which devices said printer is allowed to connect.

24. The system of claim 13, wherein said wireless communication link is a Bluetooth® communication link.

25. The system of claim 12, wherein said first device is a mobile device and said first device is able to communicate with said policy server over a communication link at least a segment of which is a wireless communication link.

26. The system of claim 25, wherein said wireless communication link is a cellular telephony link or a wireless local area network link.

27. The system of claim 12, wherein said second device has installed thereon a software application for use with said first device, and said policy affects how said software application operates.

28. A first device comprising:

a processor;

a first communication interface coupled to said processor and through which said first device is able to communicate with a policy server; and

a second communication interface coupled to said processor and through which said first device is able to communicate with other devices that are unable to communicate with said policy server,

wherein said first device is to collect information regarding those of said other devices with which said first device is communicating, to report said information to said policy server, to contact said policy server to request a policy for one of said other devices, to receive from said policy server a policy for said one of said other devices, and to send all or a portion of said policy to said one of said other devices.

29. The first device of claim 28, wherein said one of said other devices is a smart card reader and said policy defines under what circumstances confidential information stored at said smart card reader is deleted.

30. The first device of claim 28, wherein said one of said other devices is a smart card reader and said policy defines with which devices other than said first device said smart card reader is allowed to communicate.

31. The first device of claim 28, wherein said one of said other devices is a smart card reader and said policy defines the number of incorrect smart card login attempts following which said smart card reader is to be locked.

32. The first device of claim 28, wherein said one of said other devices is a smart card reader and said policy defines which algorithms said smart card reader is allowed to use to protect a communication link with said first device.

33. The first device of any one of claims 28 to 32, wherein said first communication interface is compatible with a first wireless communication standard and said second communication interface is compatible with a second, different wireless communication standard.

34. The first device of claim 33, wherein said first communication standard is a wireless local area network standard or a cellular telephony standard.

35. The first device of claim 33 or claim 34, wherein said second communication standard is the Bluetooth® standard.

36. The first device of any one of claims 33 to 34, wherein said first device is to send a confirmation to said policy server once all or a portion of said policy is applied at said one of said other devices.

37. A method in a first device, the method comprising:

collecting information regarding other devices with which said first device is communicating and which are unable to communicate with a policy server;

reporting said information to said policy server;

contacting said policy server to request a policy for one of said other devices;

receiving from said policy server said policy at said first device; and

transmitting all or a portion of said policy from said first device to said one of said other devices.

38. The method of claim 37, wherein said one of said other devices is a smart card reader and said policy defines under what circumstances confidential information stored at said smart card reader is deleted.

39. The method of claim 37, wherein said one of said other devices is a smart card reader and said policy defines with which devices other than said first device said smart card reader is allowed to communicate.

40. The method of claim 37, wherein said one of said other devices is a smart card reader and said policy defines the number of incorrect smart card login attempts following which said smart card reader is to be locked.

41. The method of claim 37, wherein said one of said other devices is a smart card reader and said policy defines which algorithms said smart card reader is allowed to use to protect a communication link with said first device.

42. The method of any one of claims 37 to 41, wherein receiving said policy at said first device comprises at least:

receiving said policy from said policy server over a communication link at least a segment of which is a wireless communication link.

43. The method of any one of claims 37 to 42, wherein receiving said policy at said first device comprises at least:

receiving said policy at a communication interface of said first device that is compatible with a cellular telephony standard or a wireless local area network standard.

44. The method of any one of claims 37 to 43, wherein transmitting all or a portion of said policy comprises at least:

transmitting all or a portion of said policy from a communication interface of said first device that is compatible with the Bluetooth® standard.

45. The method of any one of claims 37 to 44, further comprising:

sending a confirmation to said policy server once all or a portion of said policy is applied at said one of said other devices.

46. A method in a first device that is able to communicate with a policy server and is able to communicate with a second device, the method comprising:

receiving at said first device a policy pushed from said policy server, where said policy is for said second device; and

pushing said policy from said first device to said second device,

wherein said second device is unable to communicate with said policy server.

47. The method of claim 46, wherein receiving said policy at said first device comprises at least:

receiving said policy from said policy server over a communication link at least a segment of which is a wireless communication link.

48. The method of claim 46 or claim 47, wherein receiving said policy at said first device comprises at least:

receiving said policy at a communication interface of said first device that is compatible with a cellular telephony standard or a wireless local area network standard.

49. The method of any one of claims 46 to 48, wherein pushing said policy comprises:

pushing said policy from a communication interface of said first device that is compatible with the Bluetooth® standard.

50. A machine readable medium comprising executable code which, when executed in a processor of the device of any one of claims 28 to 36, causes said device to implement the steps of the method of any one of claims 37 to 45.

51. A communications system comprising the system of any one of claims 1 to 11 and/or at least one device of any one of claims 28 to 36.

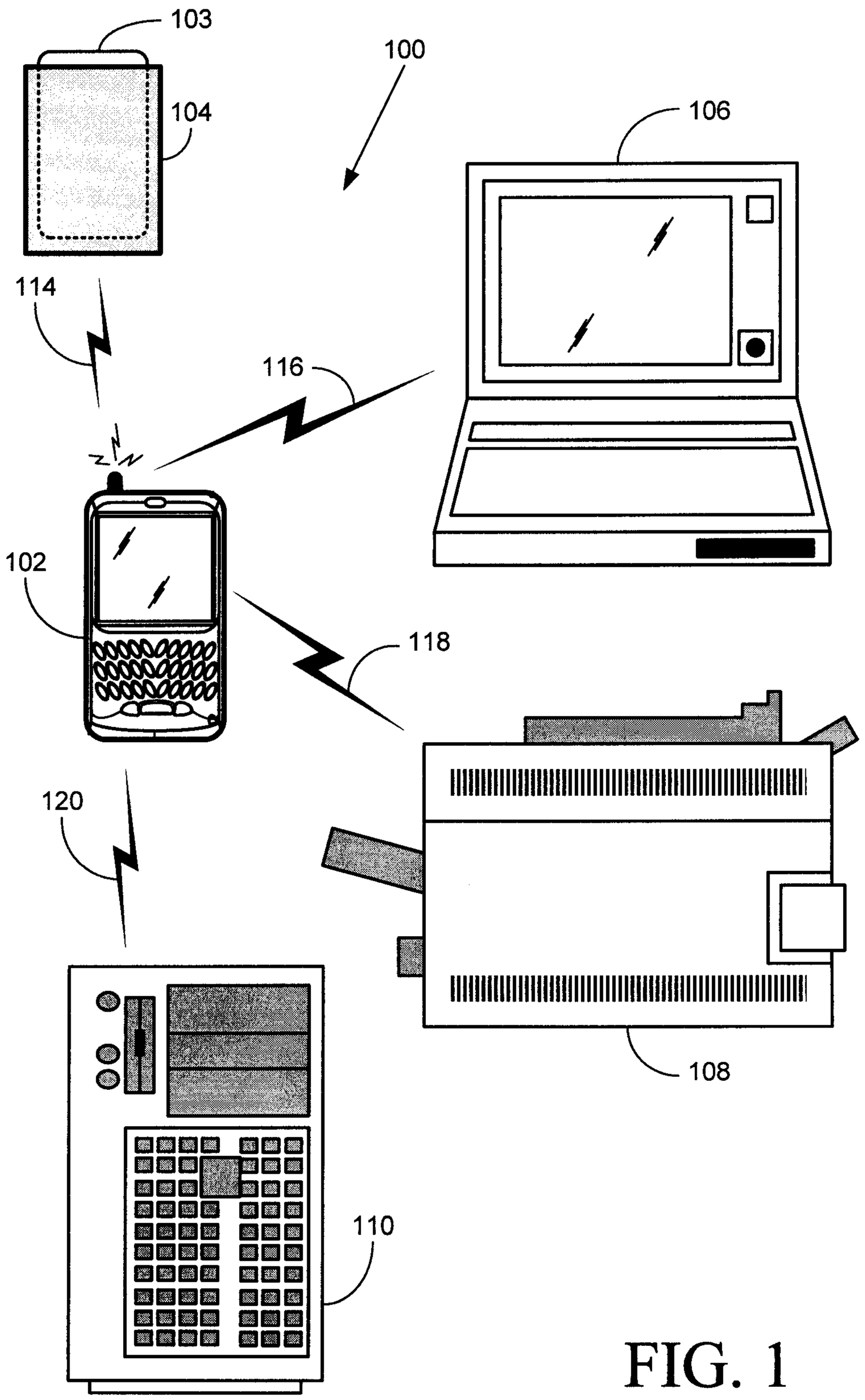


FIG. 1

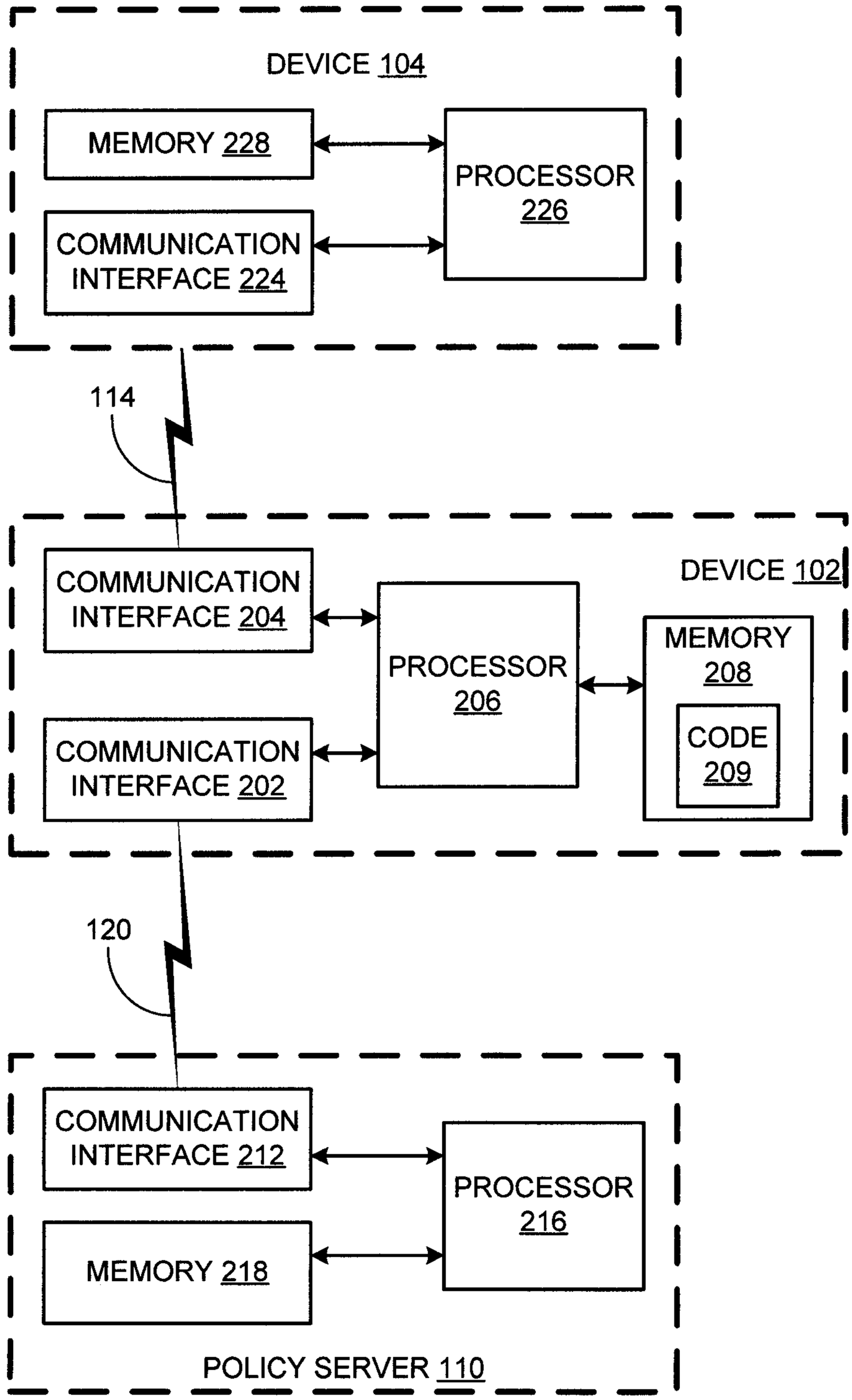

DEVICE 104
MEMORY 228
PROCESSOR 226
COMMUNICATION INTERFACE 224
114
COMMUNICATION INTERFACE 204
DEVICE 102
PROCESSOR 206
MEMORY 208
CODE 209
COMMUNICATION INTERFACE 202
120
COMMUNICATION INTERFACE 212
PROCESSOR 216
MEMORY 218
POLICY SERVER 110

FIG. 2

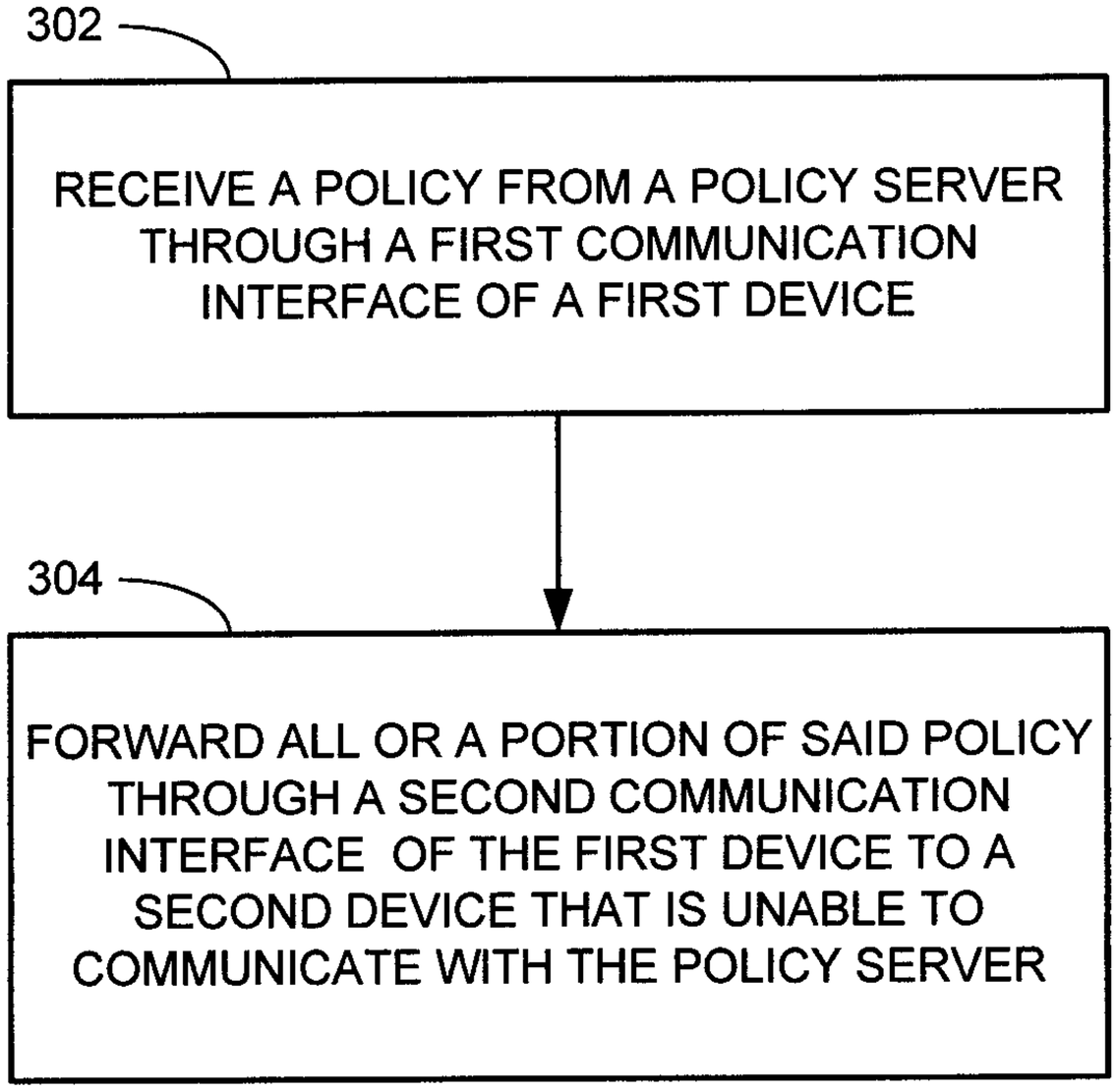

302
RECEIVE A POLICY FROM A POLICY SERVER THROUGH A FIRST COMMUNICATION INTERFACE OF A FIRST DEVICE
304
FORWARD ALL OR A PORTION OF SAID POLICY THROUGH A SECOND COMMUNICATION INTERFACE OF THE FIRST DEVICE TO A SECOND DEVICE THAT IS UNABLE TO COMMUNICATE WITH THE POLICY SERVER

FIG. 3

302

RECEIVE A POLICY FROM A POLICY SERVER THROUGH A FIRST COMMUNICATION INTERFACE OF A FIRST DEVICE

304

FORWARD ALL OR A PORTION OF SAID POLICY THROUGH A SECOND COMMUNICATION INTERFACE OF THE FIRST DEVICE TO A SECOND DEVICE THAT IS UNABLE TO COMMUNICATE WITH THE POLICY SERVER