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

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2787977 C 2016/11/29

(11)(21) **2 787 977**

(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:** 2016/11/29

(62) **Demande originale/Original Application:** 2 539 998

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

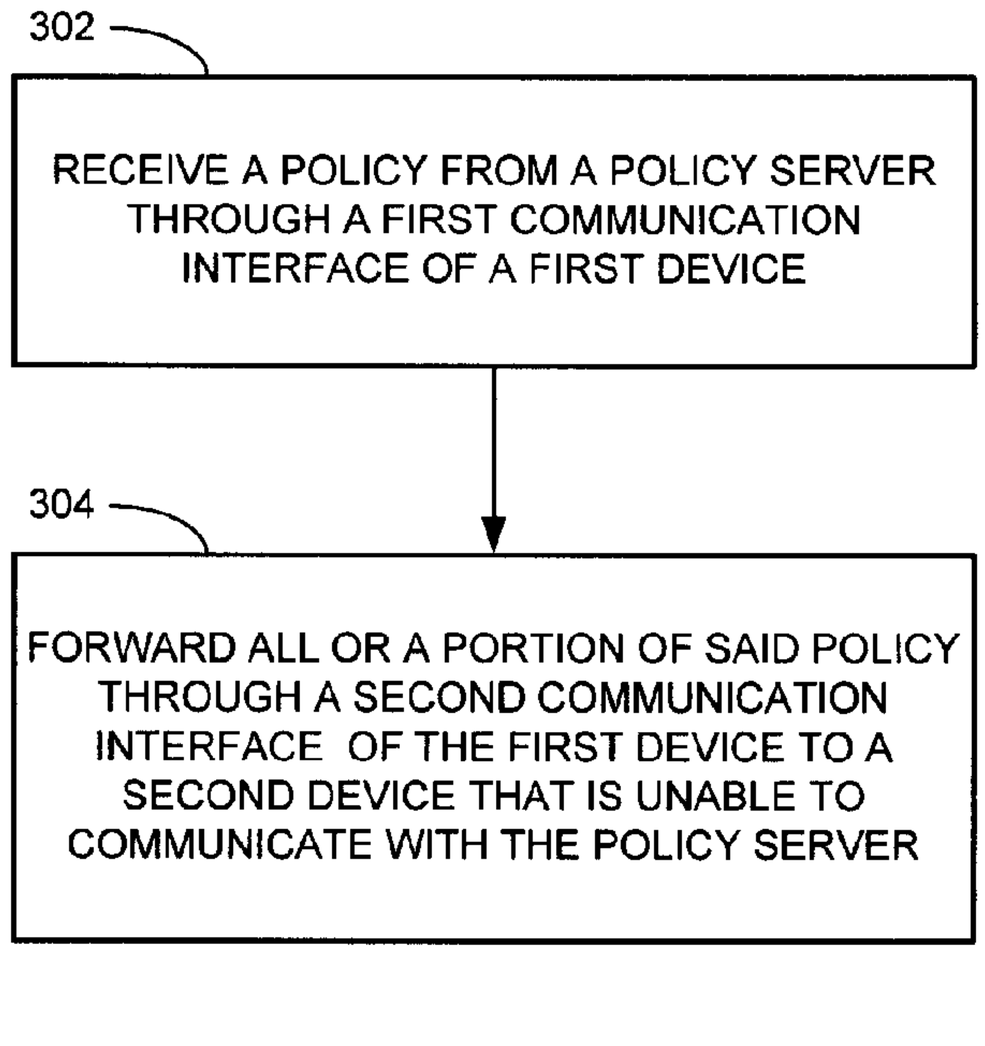
(51) **Cl.Int./Int.Cl.** ***H04L 12/24*** (2006.01), ***H04W 24/04*** (2009.01), ***H04W 84/18*** (2009.01)

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

(73) **Propriétaire/Owner:**
BLACKBERRY 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. Alternatively, no request is made and the policy server pushes 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. The first device may confirm to the policy server that all or a portion of the policy has been applied at 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. Alternatively, no request is made and the policy server pushes 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. The first device may confirm to the policy server that all or a portion of the policy has been applied at the second device.

RIM017-10CA

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 method performed by a policy server, the method comprising:

receiving a request from a first electronic device via a first interface associated with the first electronic device, the request being for a policy to apply on a second electronic device that is not capable of direct communication with the policy server; and

sending the policy to the first electronic device to cause the first electronic device to transmit the policy via a second interface associated with the first electronic device to the second electronic device, the second interface being at least one of separate and distinct from the first interface.

2. The method of claim 1, further comprising:

receiving a confirmation from the first electronic device that all or a portion of the policy has been applied on the second electronic device.

3. The method of claim 1 or claim 2, wherein the first interface is compatible with a standard and the second interface is not compatible with the standard.

4. The method of any one of claims 1 to 3, wherein the first electronic device is a mobile electronic device.

5. The method of claim 4, wherein the mobile electronic device is a cellular phone, or a personal digital assistant, or an electronic mail client, or a gaming device, or a laptop computer, or a notebook computer, or a desktop computer.

6. The method of any one of claims 1 to 3, wherein the first electronic device is a server computer.

7. A policy server comprising:

a processor;

a memory coupled to the processor, the memory storing one or more policies and instructions executable by the processor, the instructions being adapted to:

receive a request from a first electronic device via a first interface associated with the first electronic device, the request being for one of the policies to apply on a second electronic device that is not capable of direct communication with the policy server; and

send the policy to the first electronic device to cause the first electronic device to transmit the policy via a second interface associated with the first electronic device to the second electronic device, the second interface being at least one of separate from and distinct from the first interface.

8. The policy server of claim 7, wherein the instructions are further adapted to:

receive from the first electronic device, via the first interface, a confirmation that all or a portion of the policy has been applied on the second electronic device.

9. The policy server of claim 7 or claim 8, wherein the first interface is compatible with a standard and the second interface is not compatible with the standard.

10. The policy server of any one of claims 7 to 9, wherein the first electronic device is a mobile electronic device.

11. The policy server of claim 10, wherein the mobile electronic device is a cellular phone, or a personal digital assistant, or an electronic mail client, or a gaming device, or a laptop computer, or a notebook computer, or a desktop computer.

12. The policy server of any one of claims 7 to 9, wherein the first electronic device is a server computer.

13. A non-transitory storage medium containing instructions, comprising:

first instructions that, when executed, cause a policy server to receive a request from a first electronic device via a first interface associated with the first electronic device, the request being for a policy to apply on a second electronic device that is not capable of direct communication with the policy server; and

second instructions that, when executed, cause the policy server to send the policy to the first electronic device for transmission of the policy by the first electronic device to the second electronic device via a second interface associated with the first electronic device, the second interface being at least one of separate from and distinct from the first interface.

14. The non-transitory storage medium of claim 13, further comprising third instructions that, when executed, cause the policy server to receive a confirmation from the first electronic device that all or a portion of the policy has been applied on the second electronic device.

15. The non-transitory storage medium of claim 13 or claim 14, wherein the first interface is compatible with a standard and the second interface is not compatible with the standard.

16. The non-transitory storage medium of any one of claims 13 to 15, wherein the first electronic device is a mobile electronic device.

17. The non-transitory storage medium of claim 16, wherein the mobile electronic device is a cellular phone, or a personal digital assistant, or an electronic mail client, or a gaming device, or a laptop computer, or a notebook computer, or a desktop computer.

18. The non-transitory storage medium of any one of claims 13 to 15, wherein the first electronic device is a server computer.

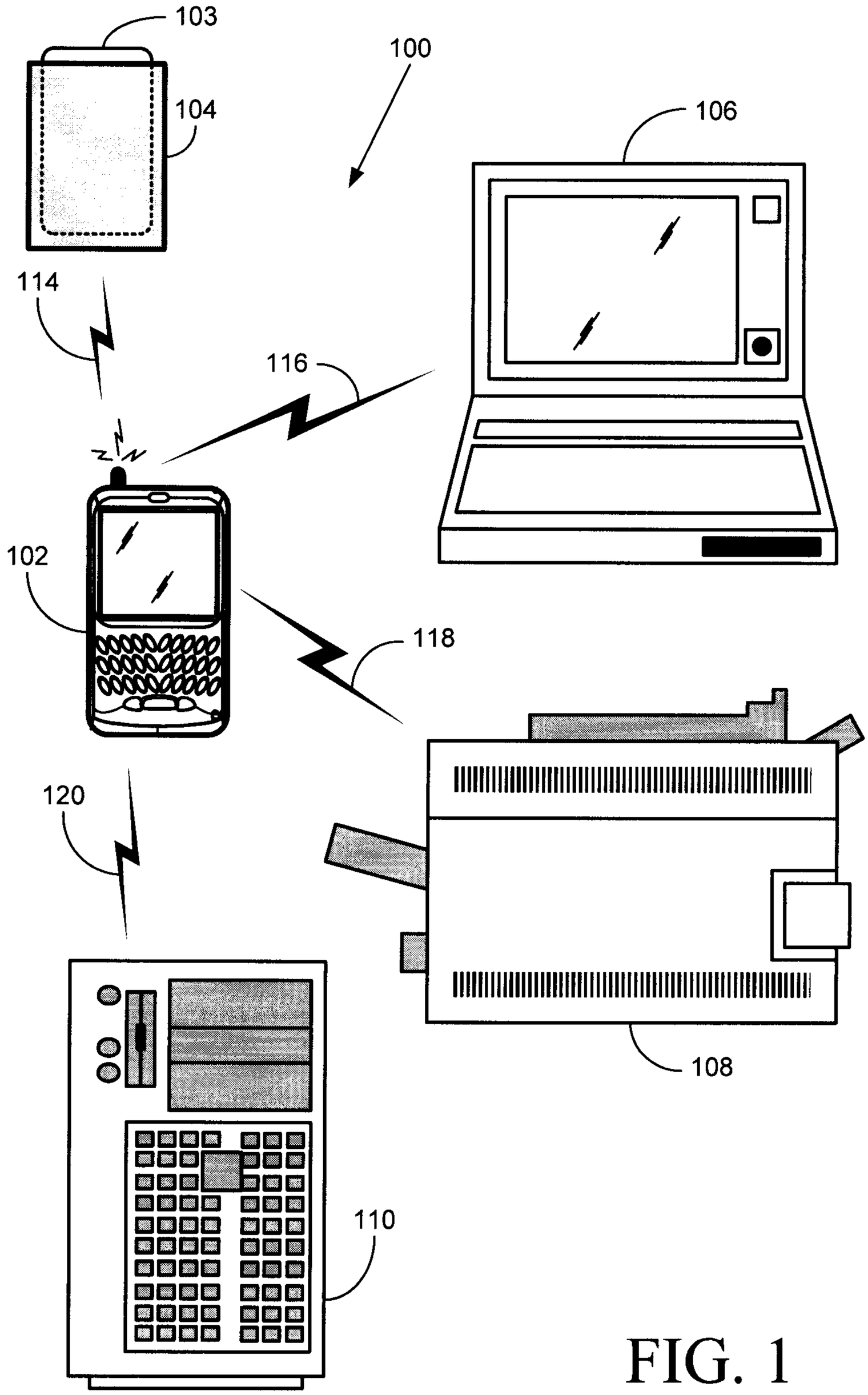


FIG. 1

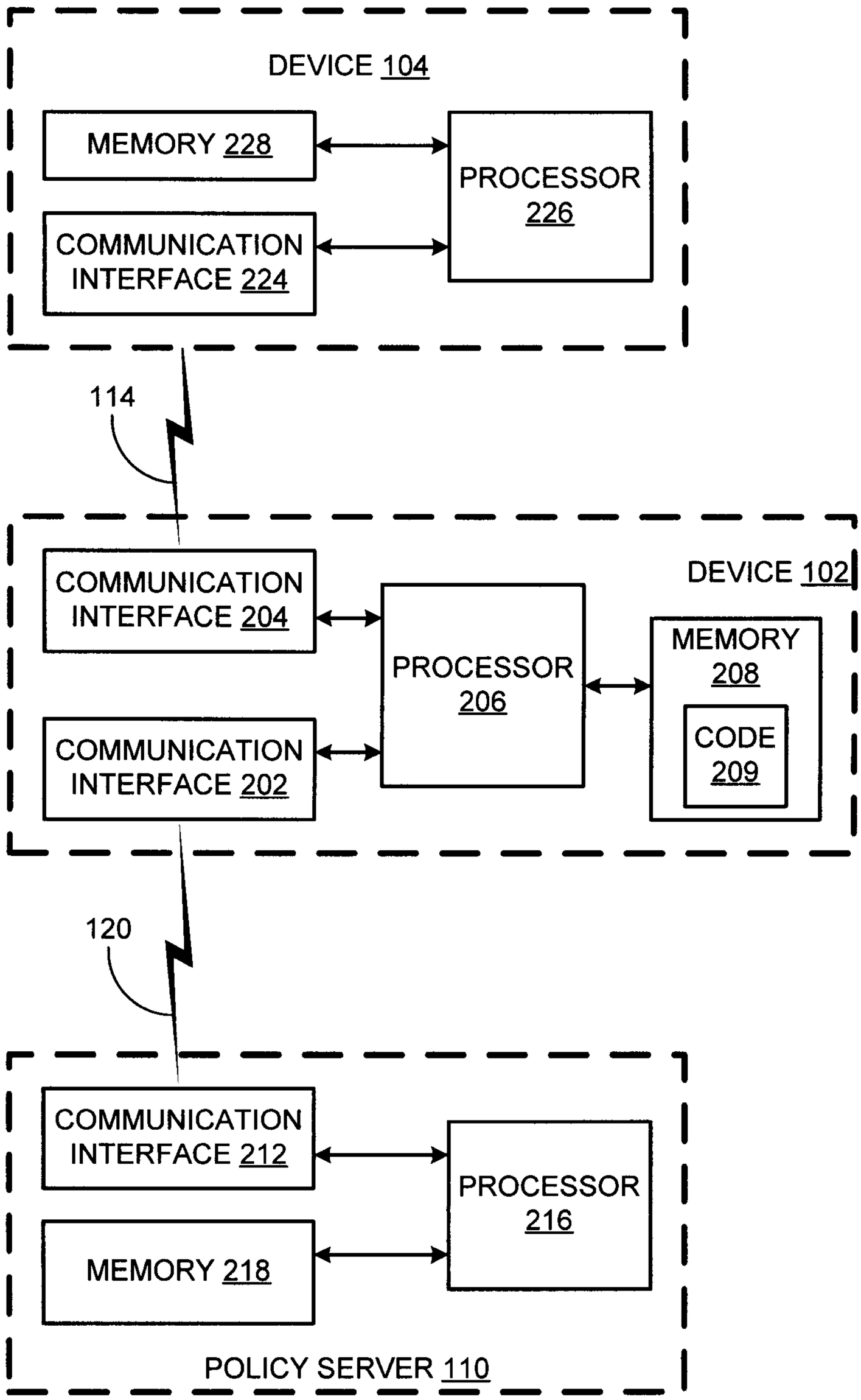

DEVICE 104
MEMORY 228
PROCESSOR 226
COMMUNICATION INTERFACE 224
114
COMMUNICATION INTERFACE 204
DEVICE 102
PROCESSOR 206
MEMORY 208
CODE 209
COMMUNICATION INTERFACE 202
120
COMMUNICATION INTERFACE 212
PROCESSOR 216
MEMORY 218
POLICY SERVER 110

FIG. 2

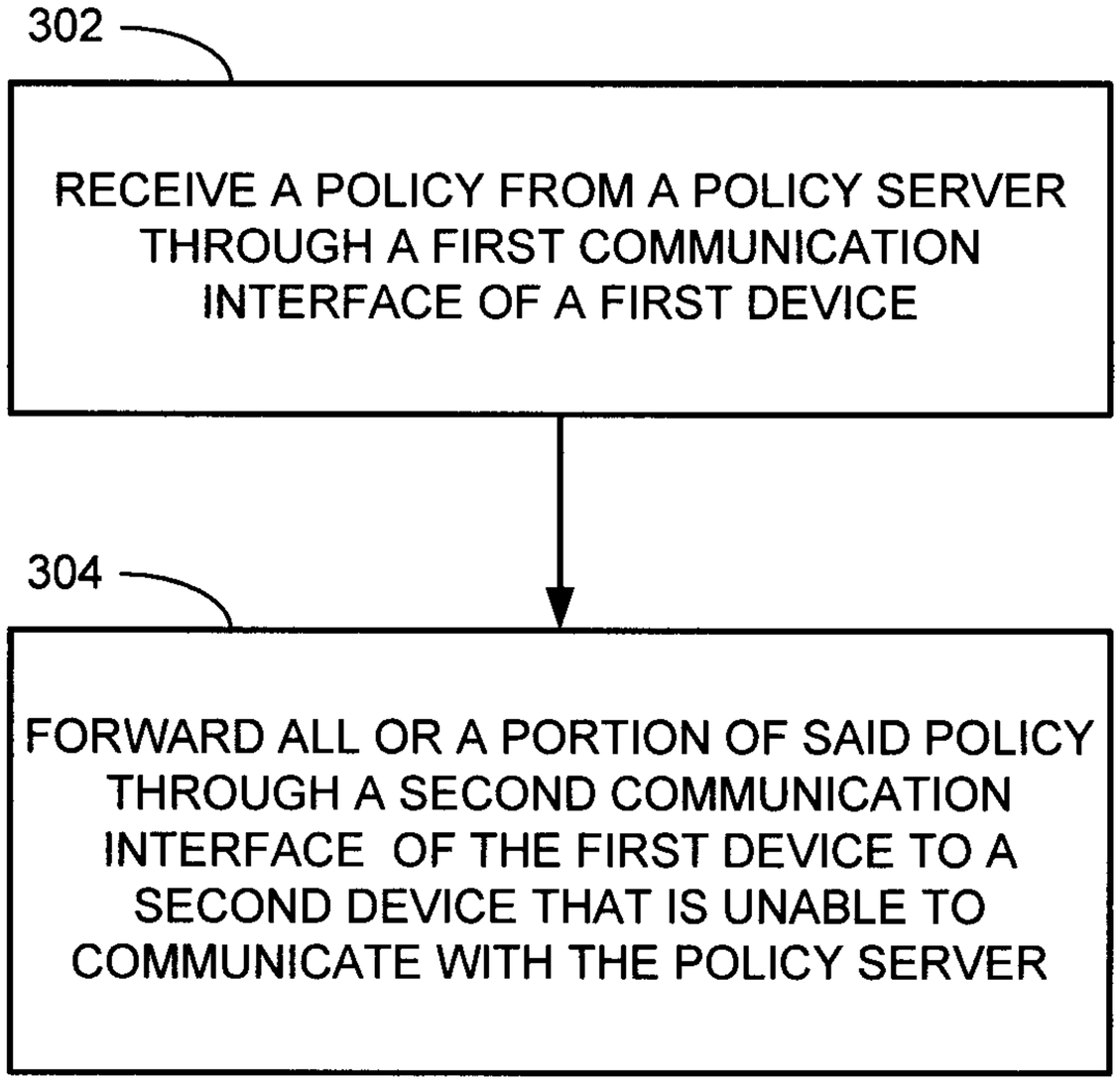
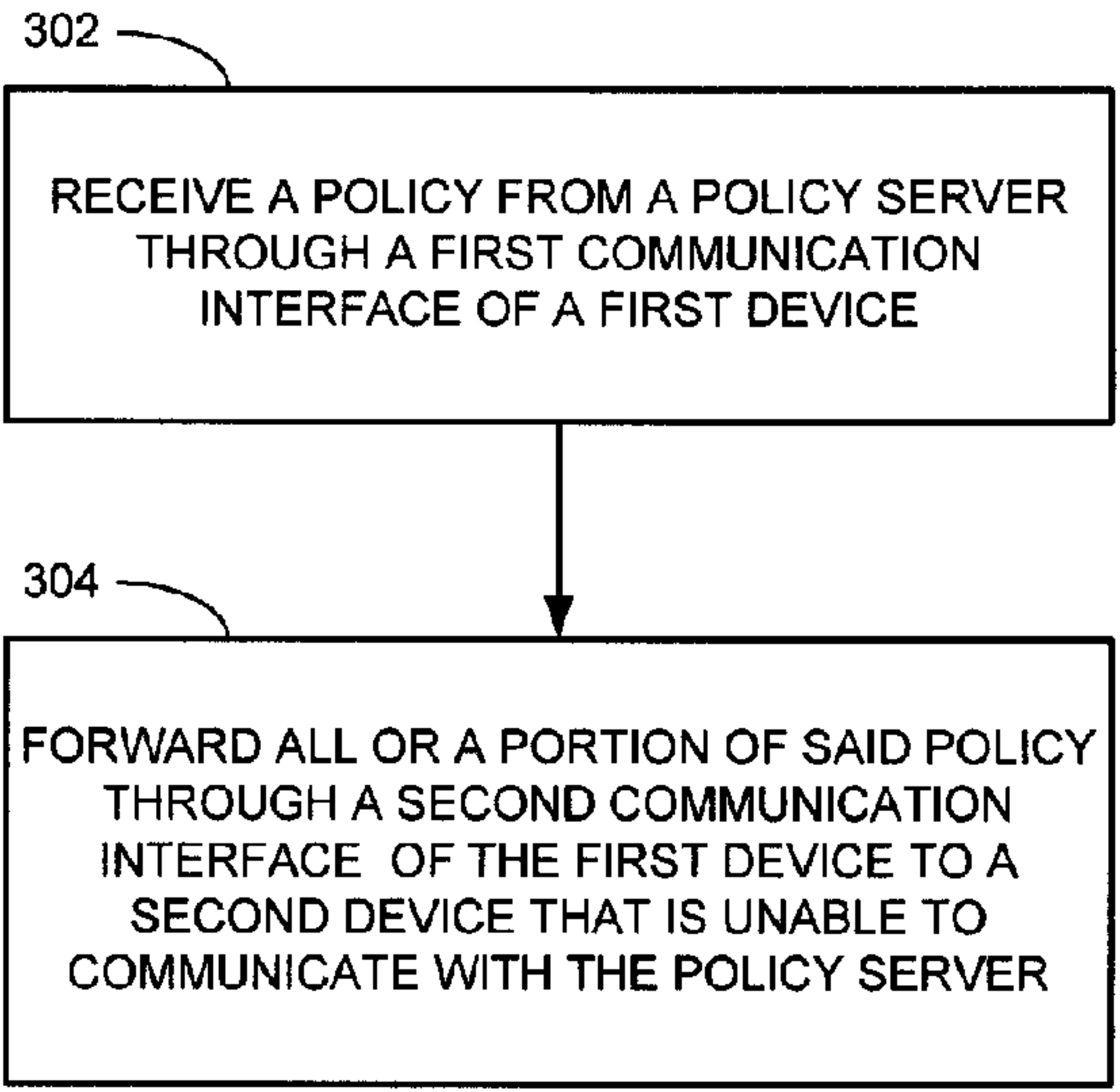

302
RECEIVE A POLICY FROM A POLICY SERVER THROUGH A FIRST COMMUNICATION INTERFACE OF A FIRST DEVICE
304
FORWARD ALL OR A PORTION OF SAID POLICY THROUGH A SECOND COMMUNICATION INTERFACE OF THE FIRST DEVICE TO A SECOND DEVICE THAT IS UNABLE TO COMMUNICATE WITH THE POLICY SERVER

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