US 20020141586A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2002/0141586 A1

Margalit et al. (43) Pub. Date: Oct. 3, 2002

(54) AUTHENTICATION EMPLOYING THE BLUETOOTH COMMUNICATION PROTOCOL

(75) Inventors: **Yanki Margalit**, Ramat Gan (IL); **Dany Margalit**, Ramat Gan (IL); **Michael Zunke**, Tel Aviv (IL)

Correspondence Address:
Ladas & Parry
26 West 61 Street
New York, NY 10023 (US)

(73) Assignee: **ALADDIN KNOWLEDGE SYSTEMS LTD.**

(21) Appl. No.: **09/821,716**

(22) Filed: **Mar. 29, 2001**

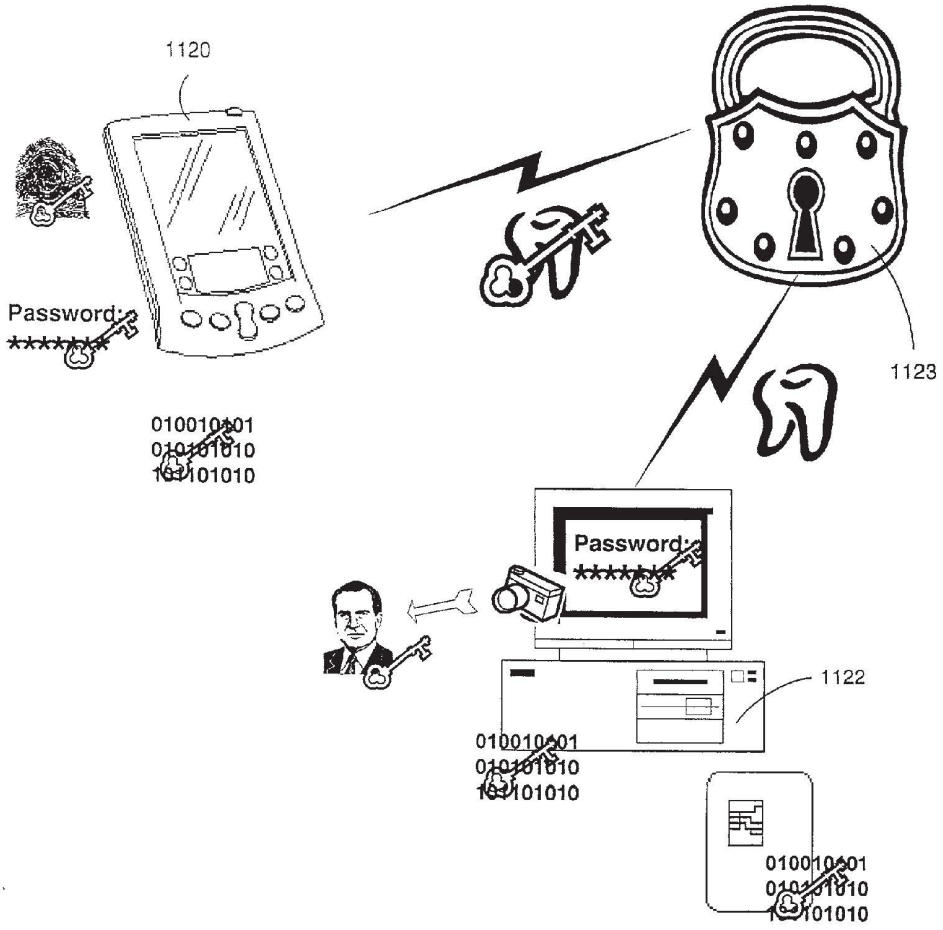
Publication Classification

(51) **Int. Cl.**[7] **H04L 9/00**

(52) **U.S. Cl.** **380/270**

(57) **ABSTRACT**

A device and method capable of communicating with a communication network via a Bluetooth communication protocol, wherein the device includes at least one authentication functionality, at least part of at least one of which is operative to communicate authentication information via the Bluetooth communication protocol.



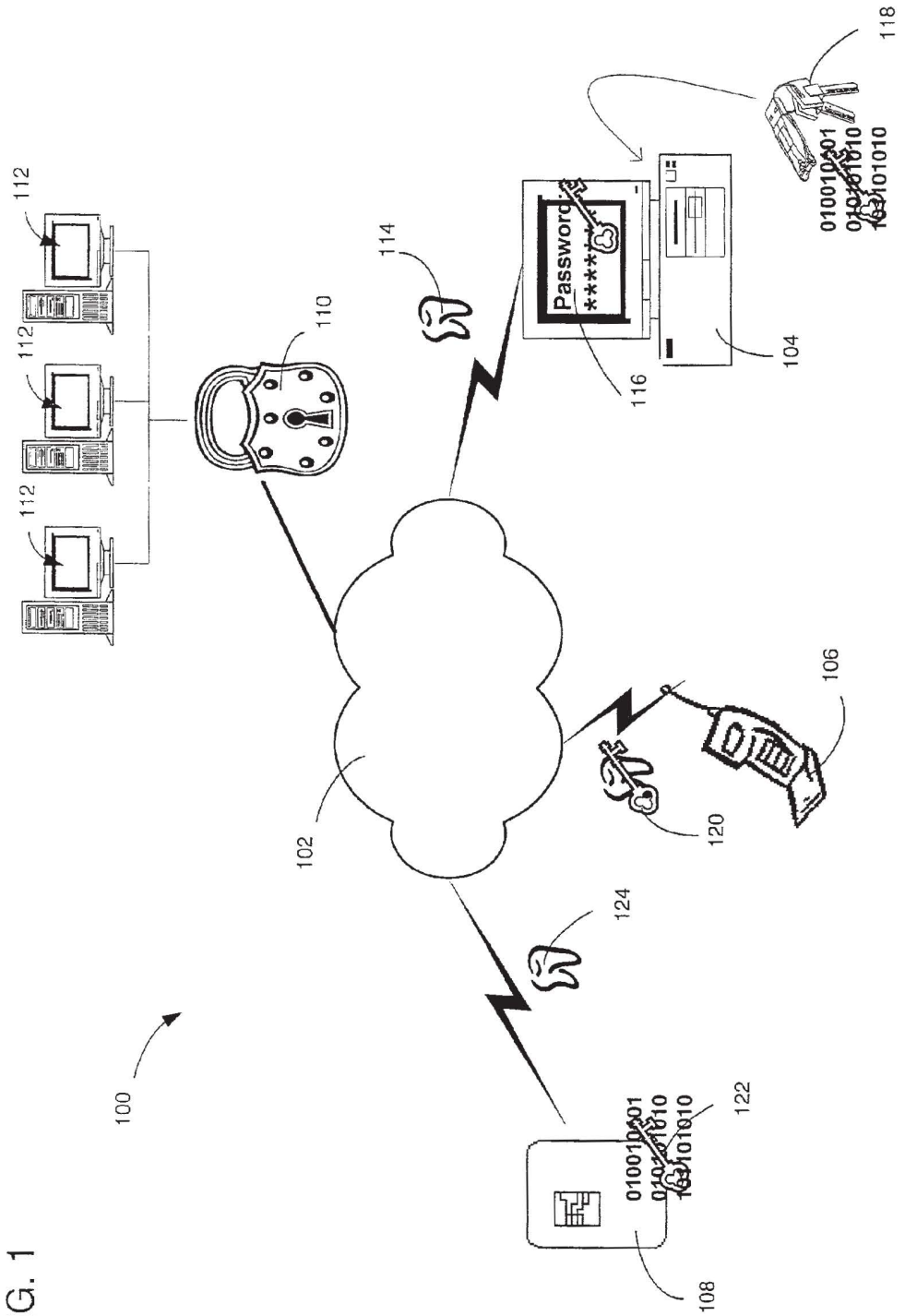

100
102
104
106
108
110
112
112
112
114
116
118
120
122
124
Password
****
01001010
01001010
01001010

FIG. 1

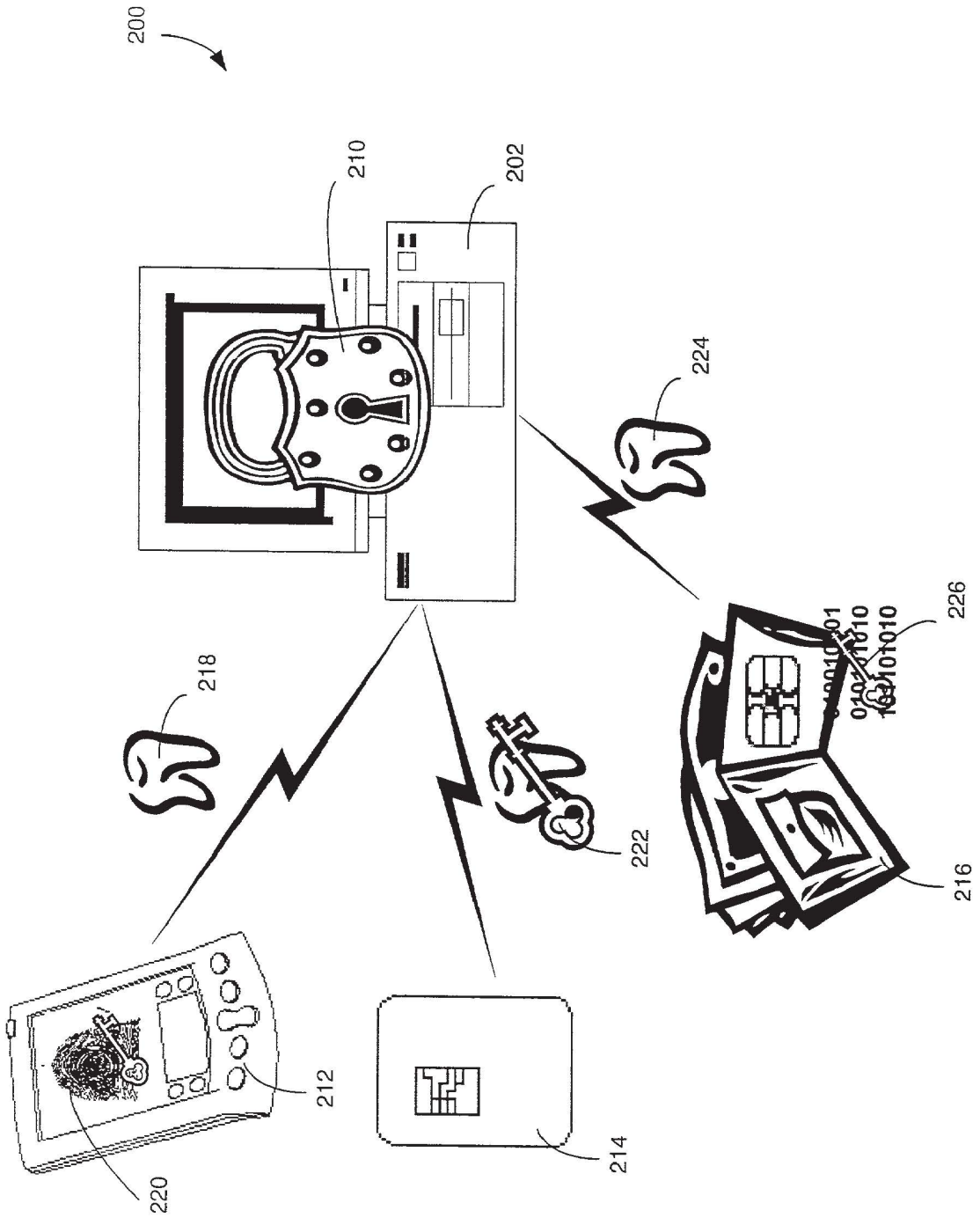


FIG. 2

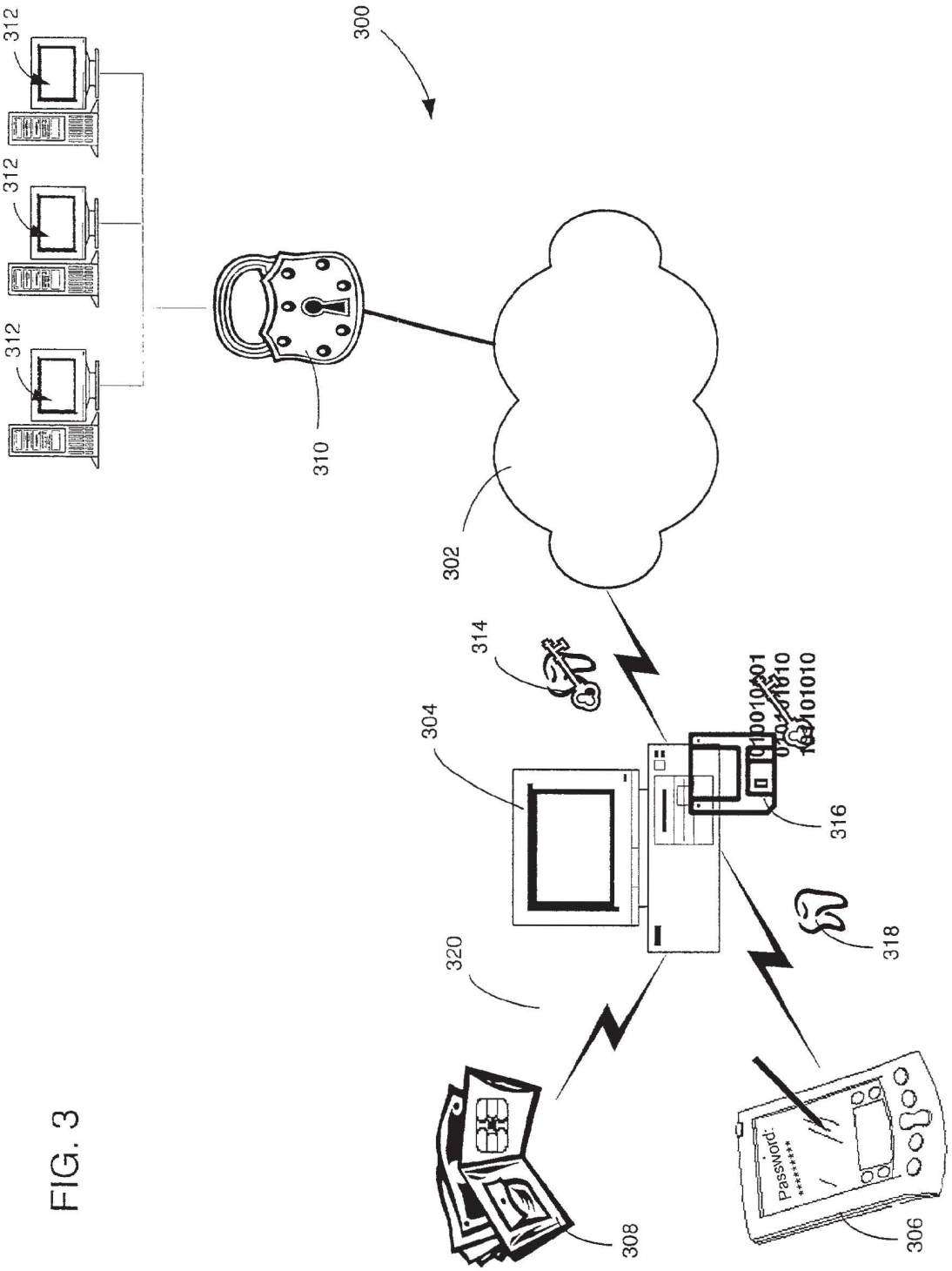


FIG. 3

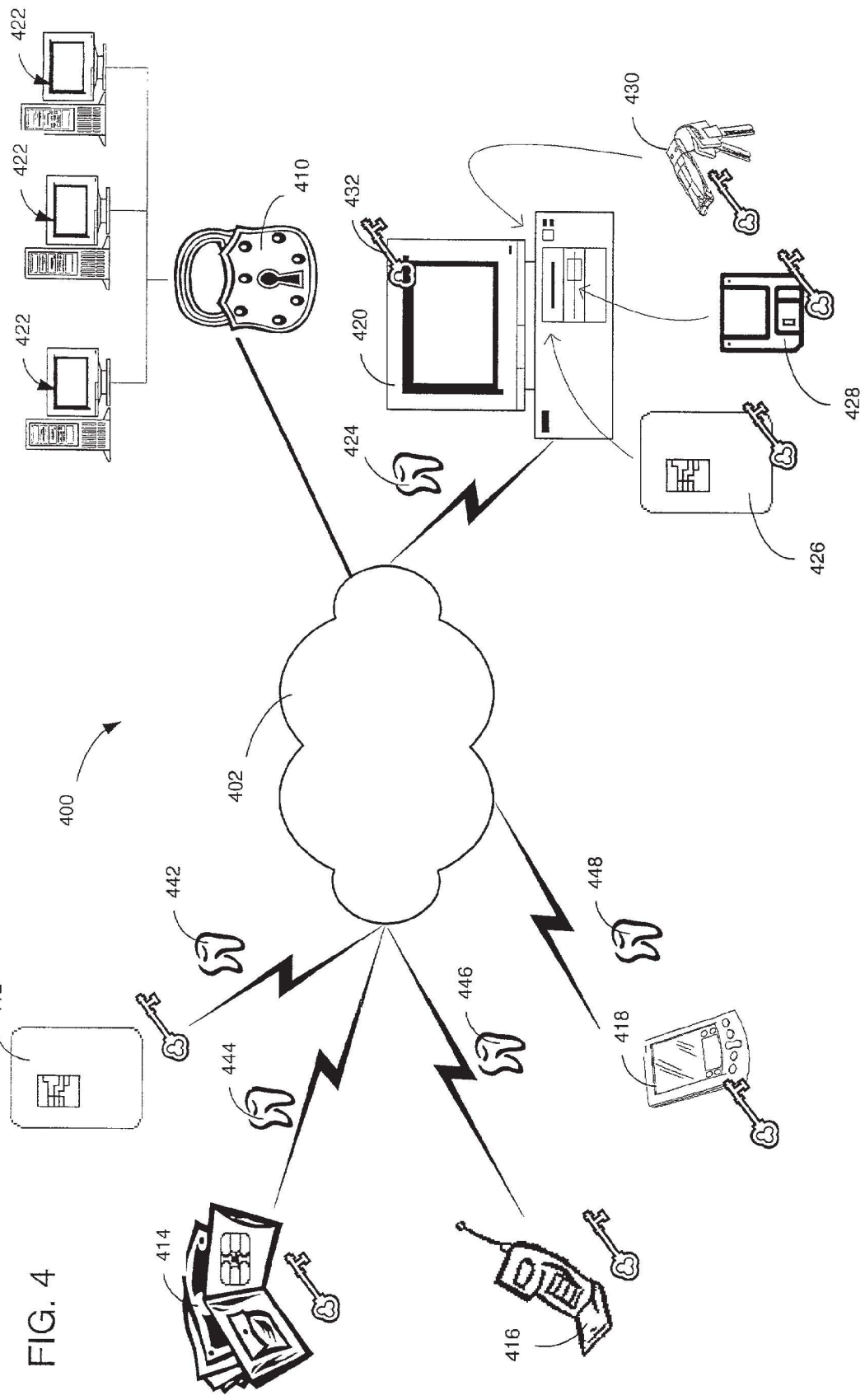

400
402
410
412
414
416
418
420
422
422
422
424
426
428
430
432
442
444
446
448

FIG. 4

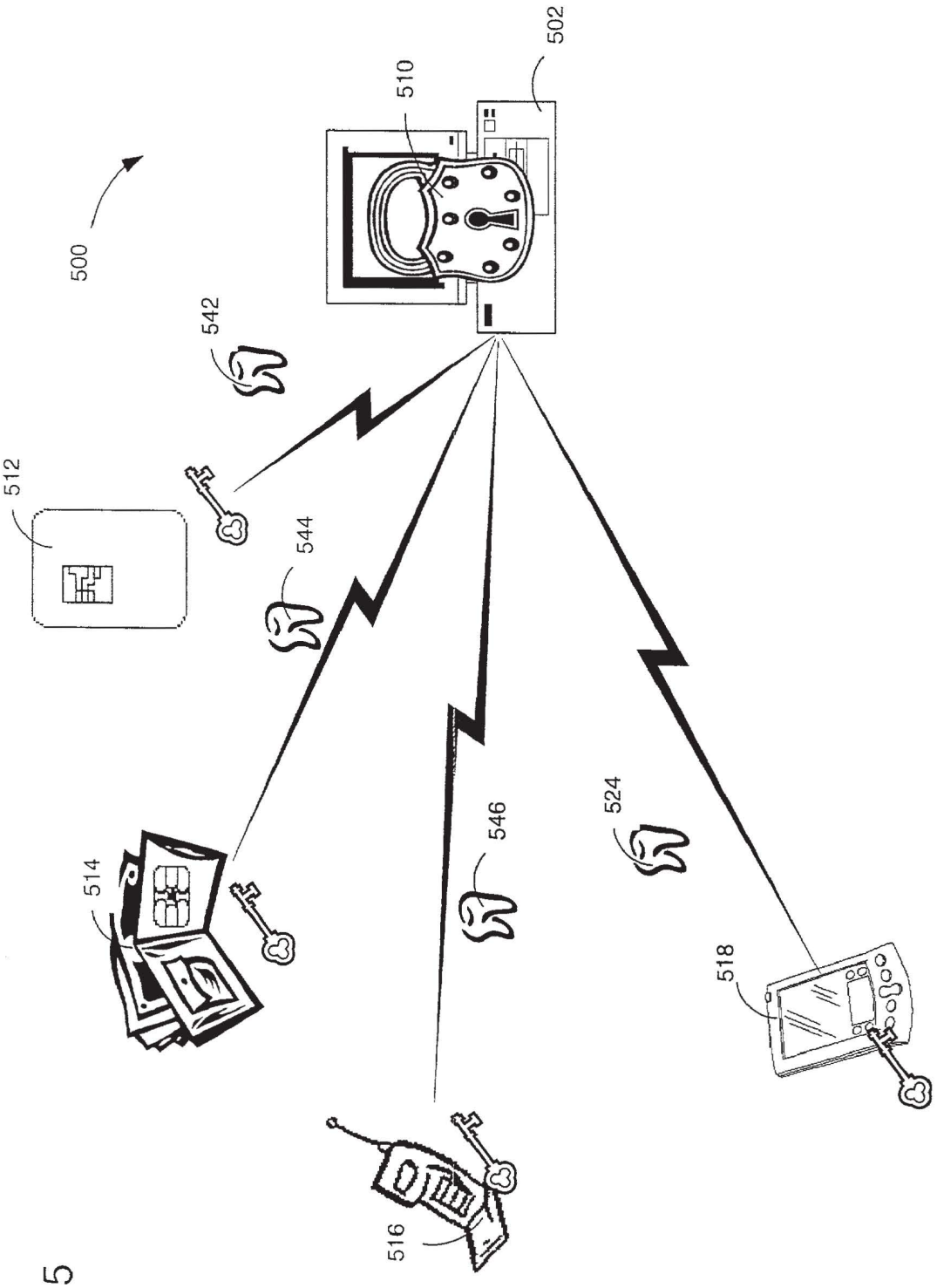


FIG. 5

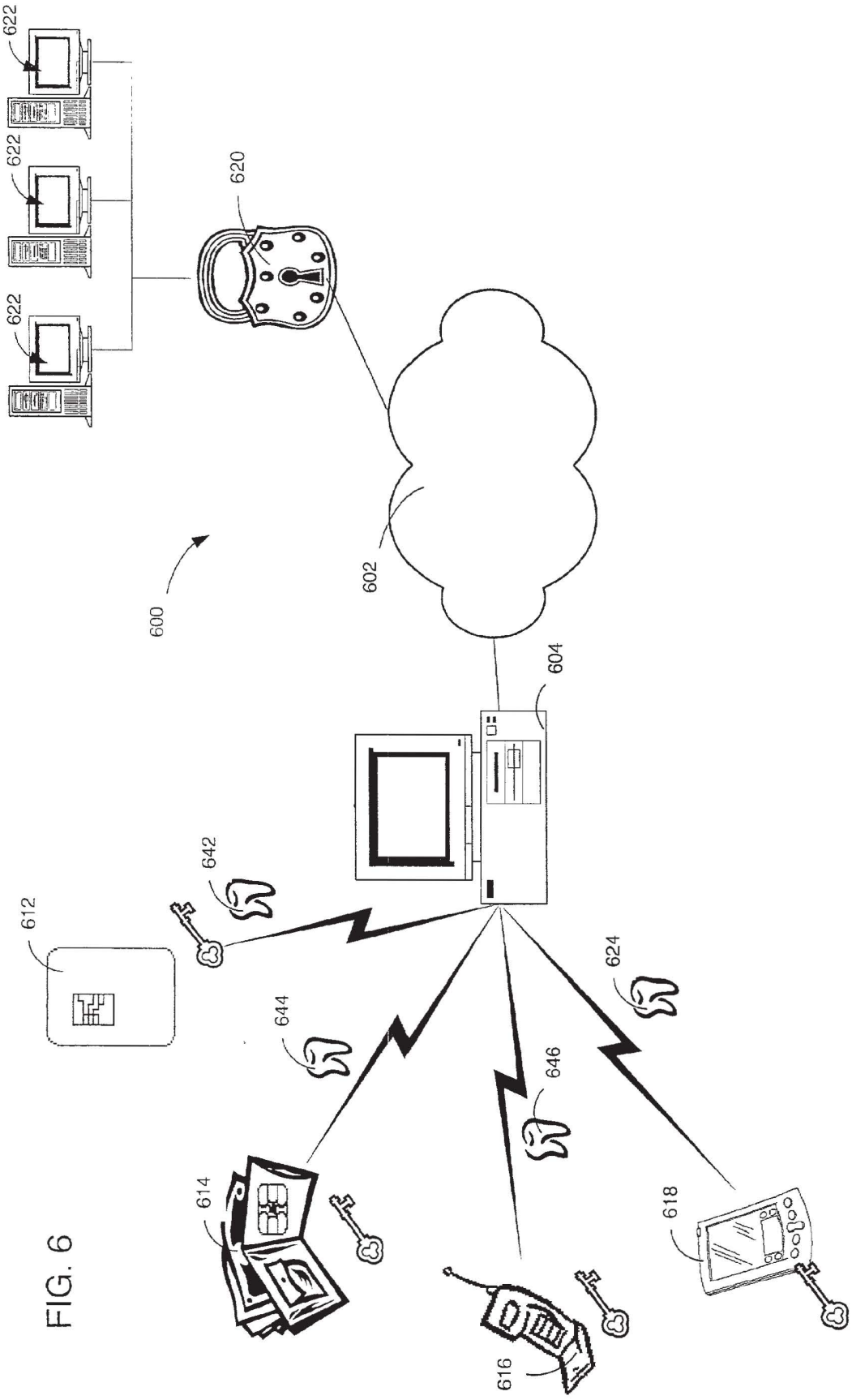


FIG. 6

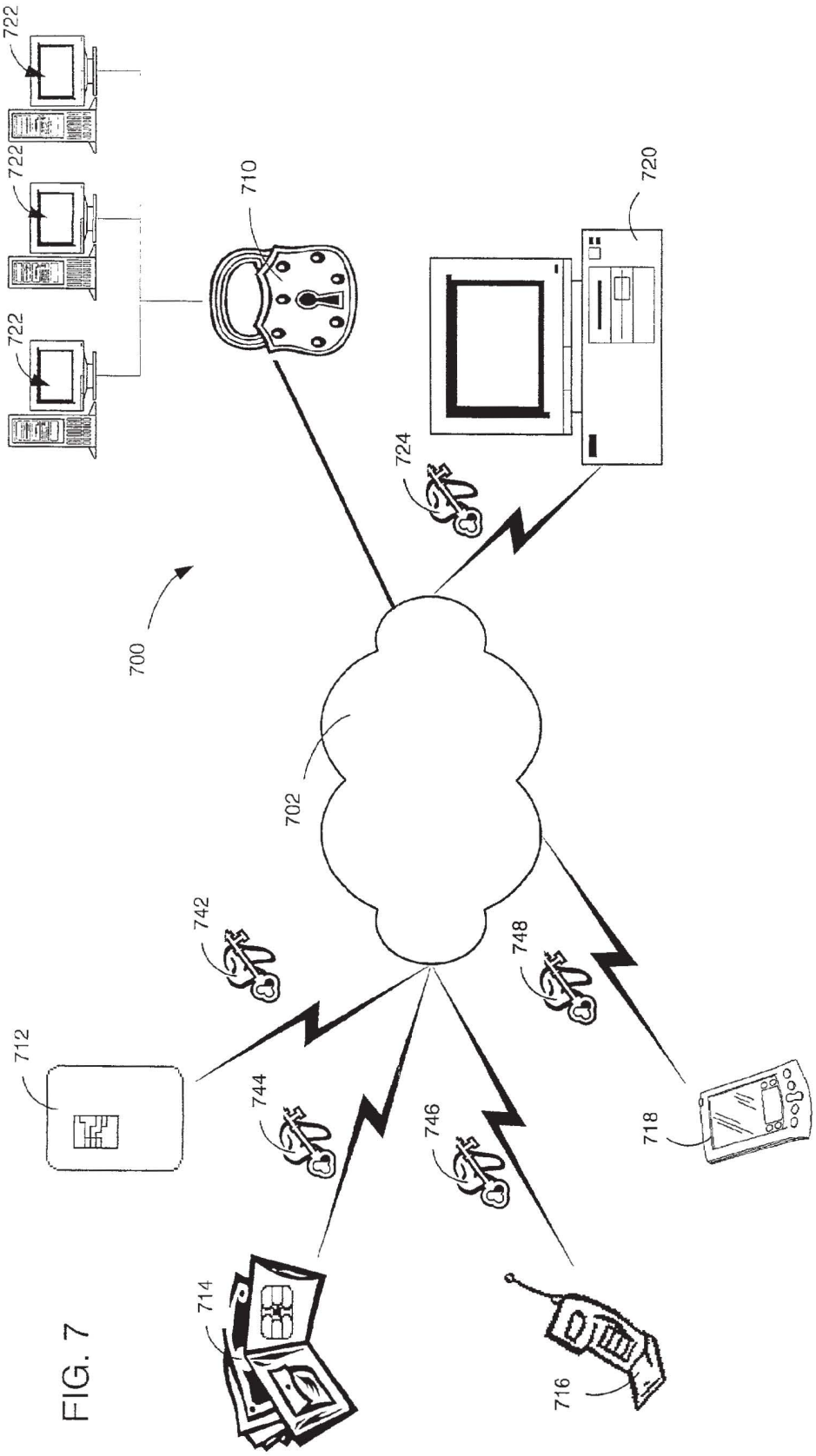


FIG. 7

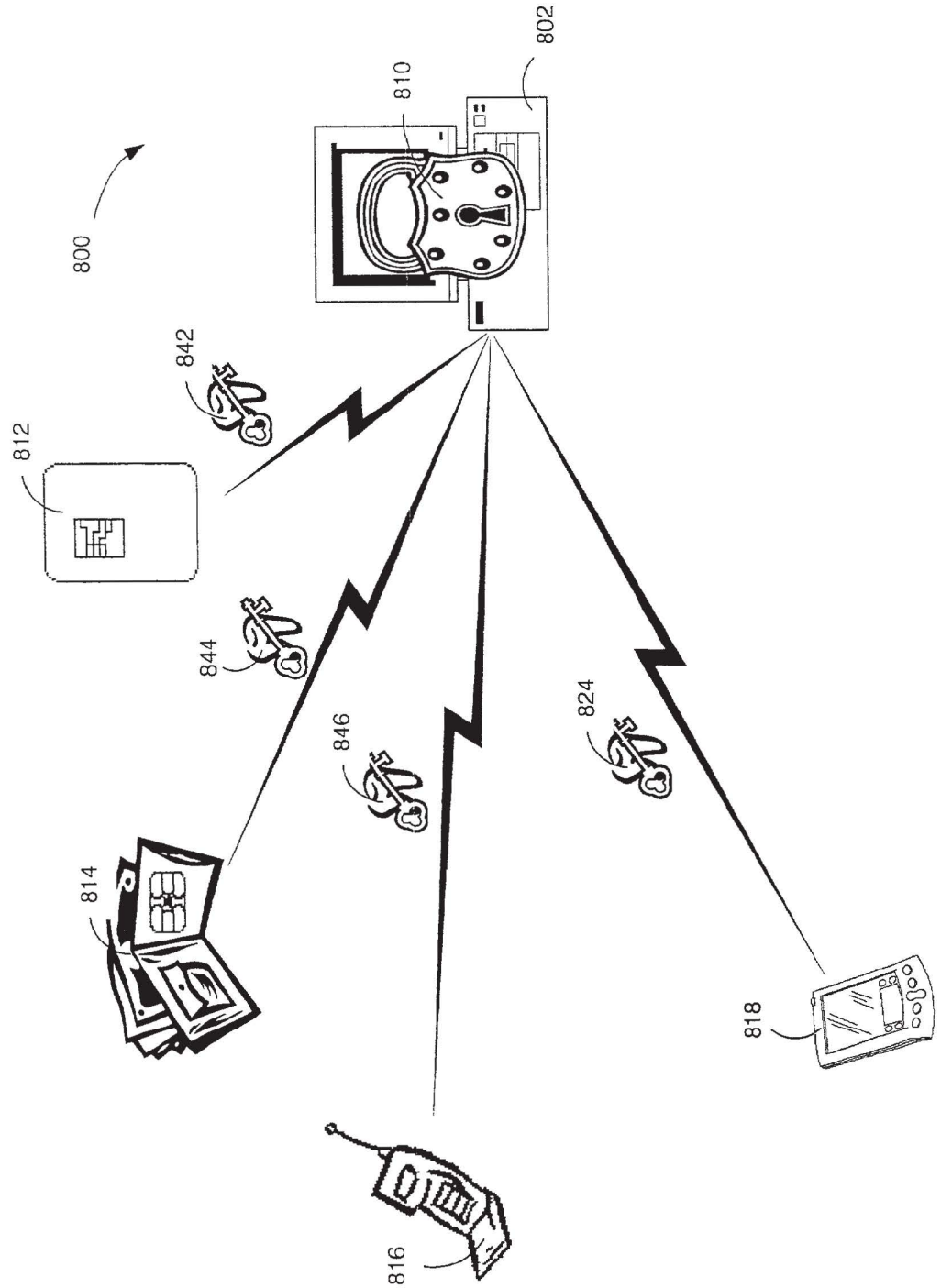


FIG. 8

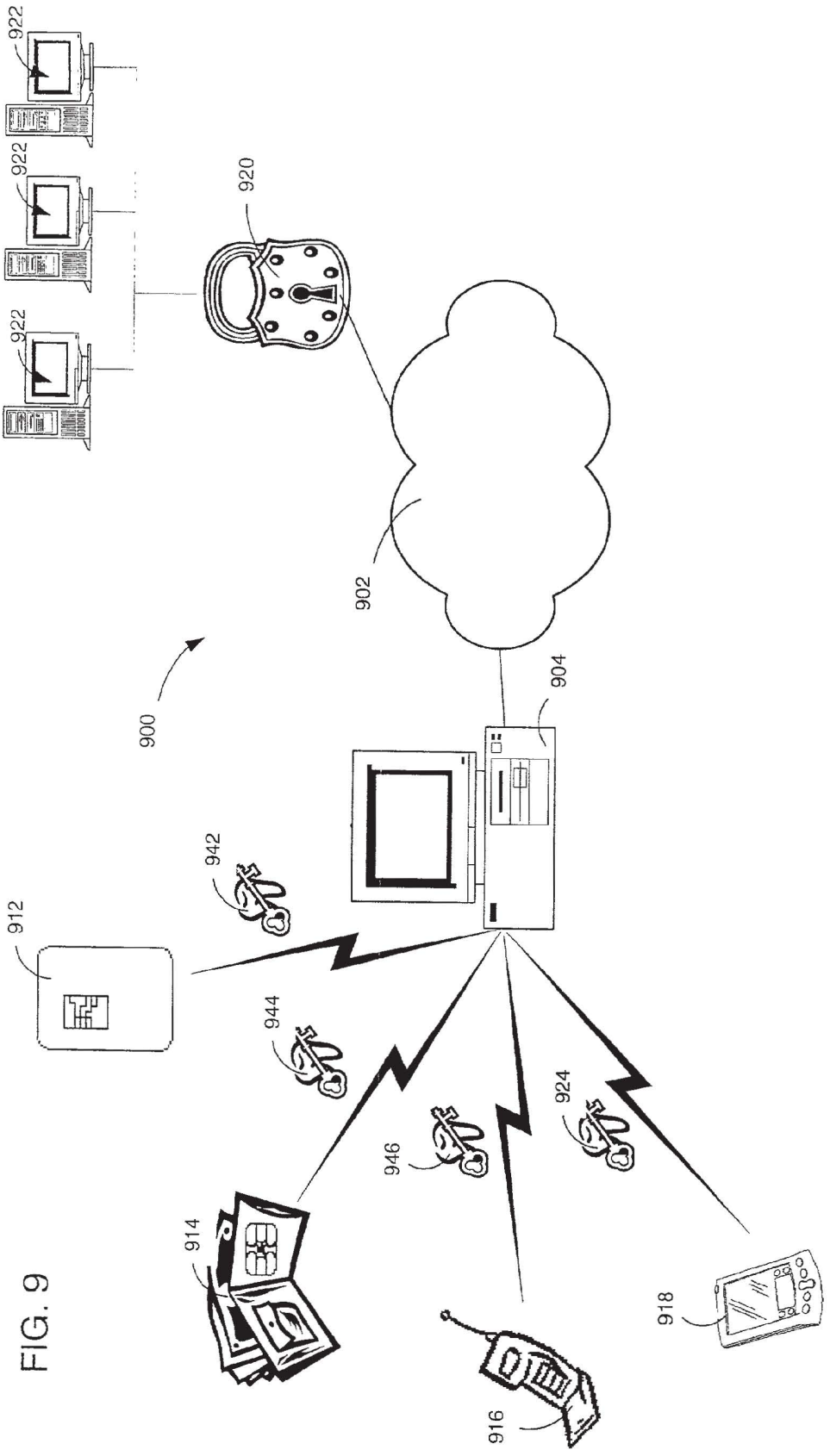


FIG. 9

FIG. 10A

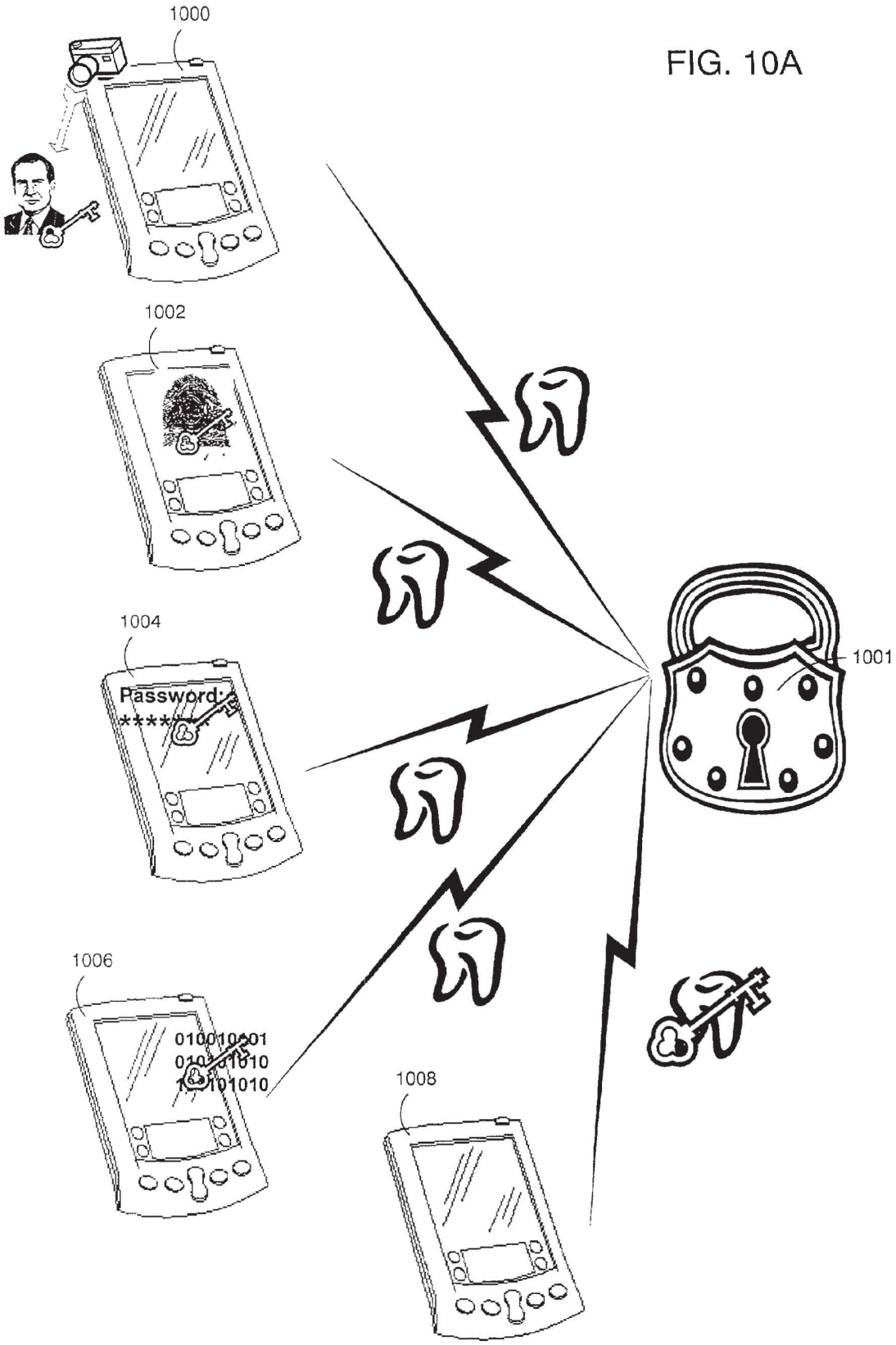


FIG. 10B

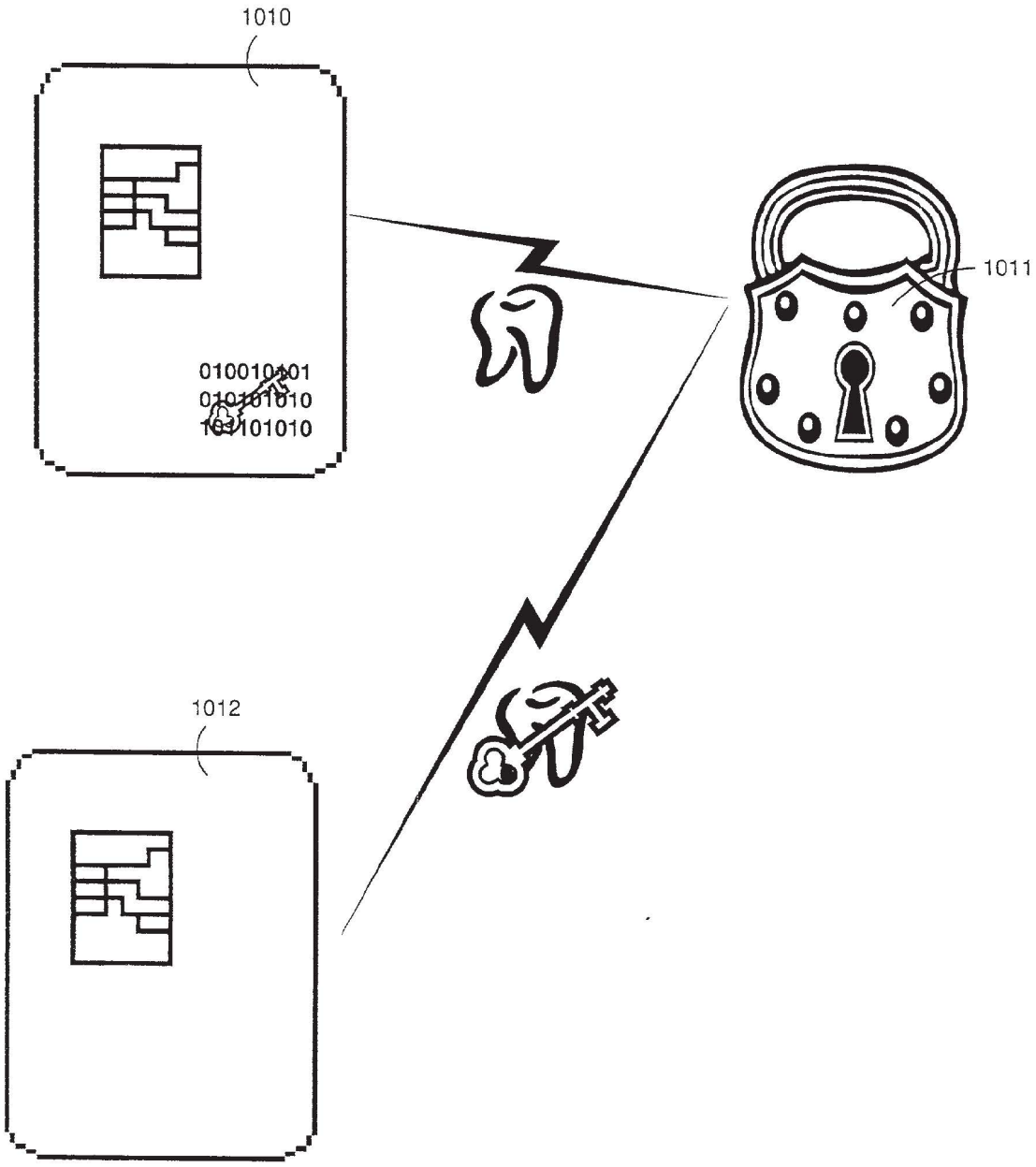


FIG. 10C

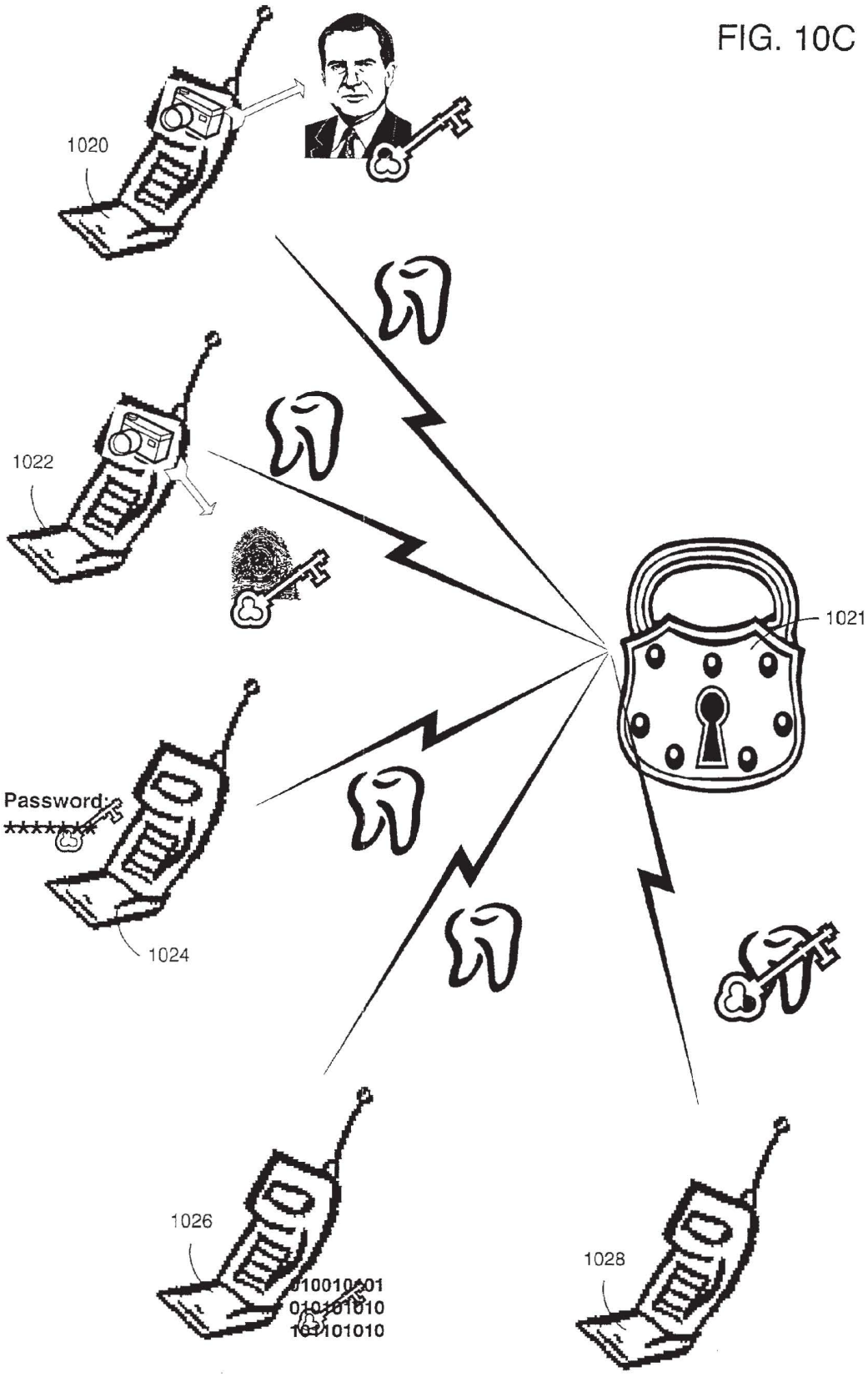


FIG. 10D

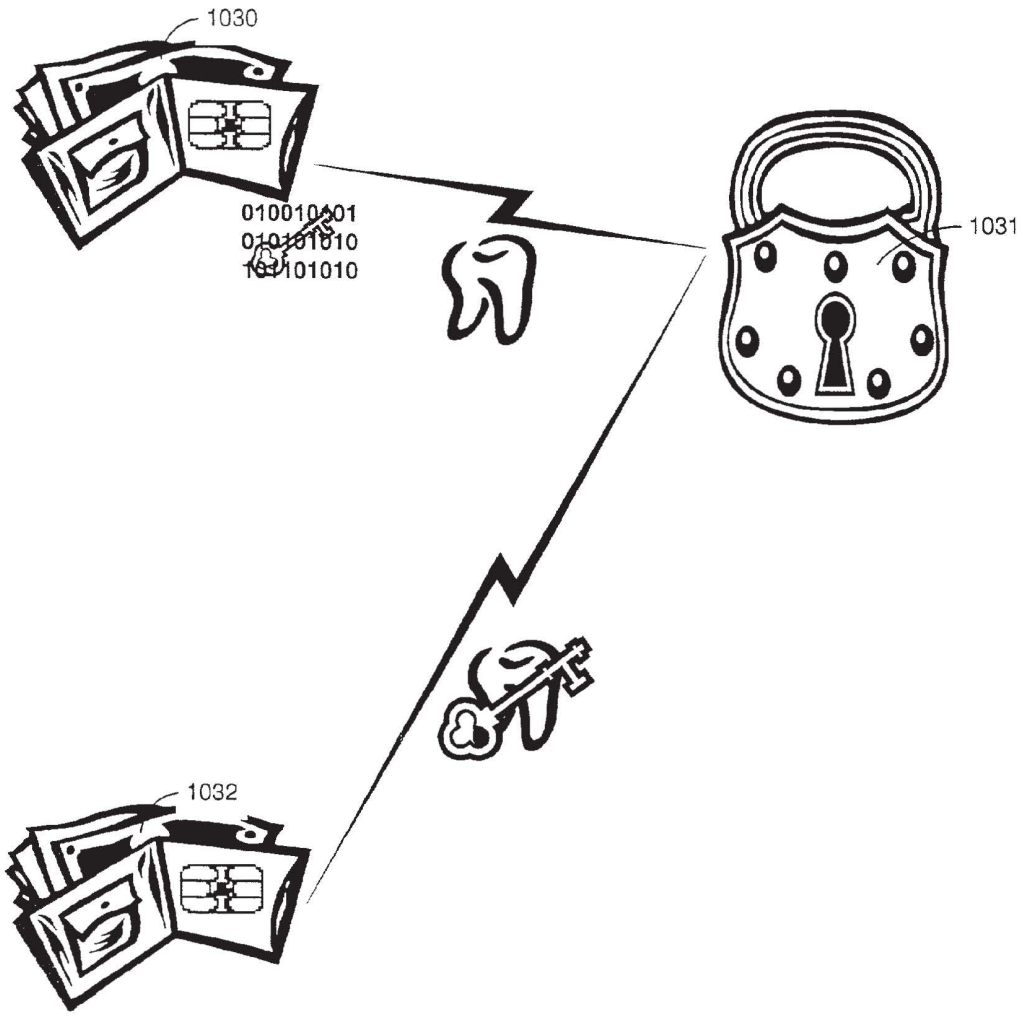


FIG. 10E

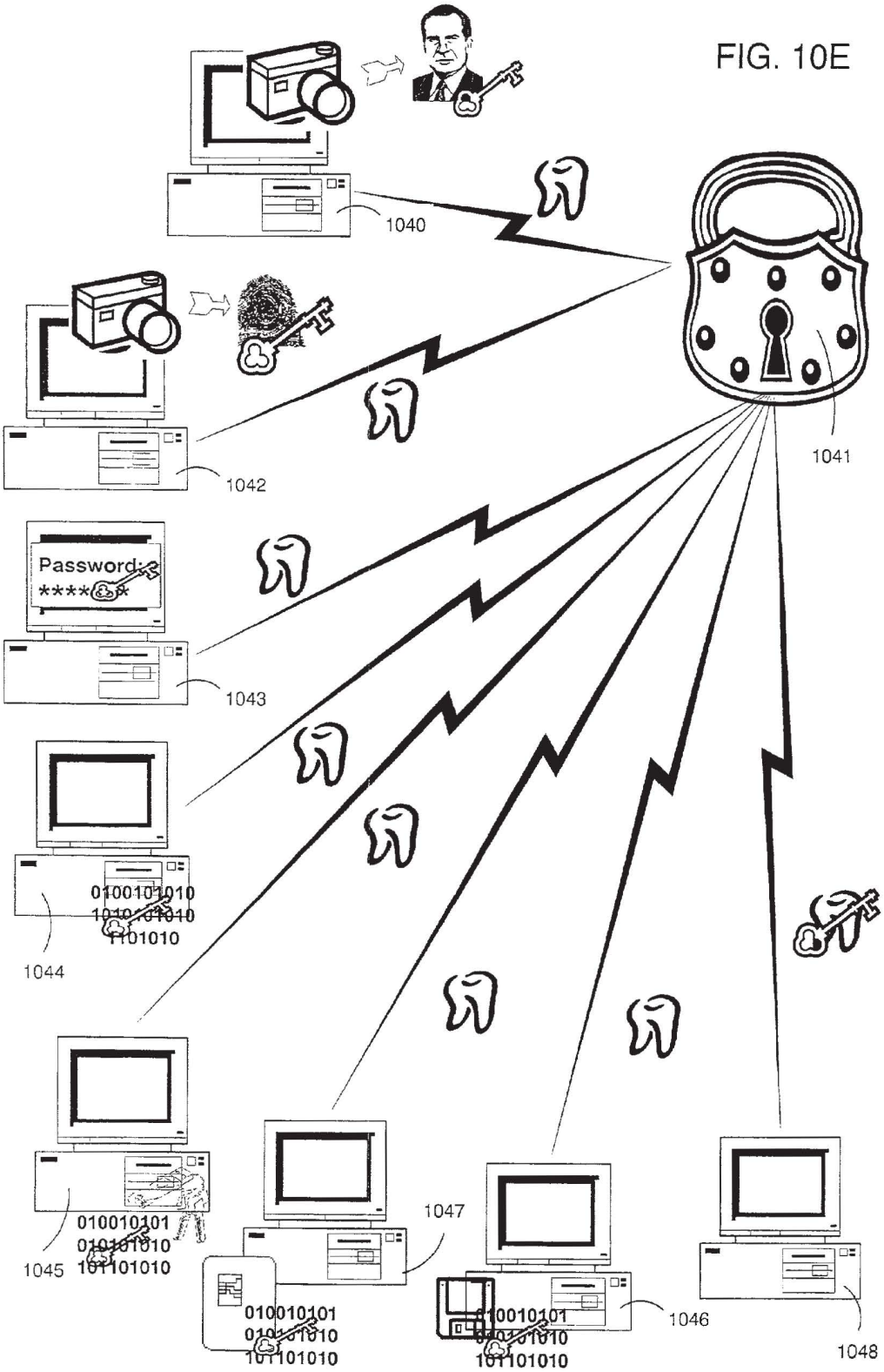

1040
1041
1042
Password:
****
1043
1044
1045
1046
1047
1048
010010101
010101010
101101010

FIG. 11A

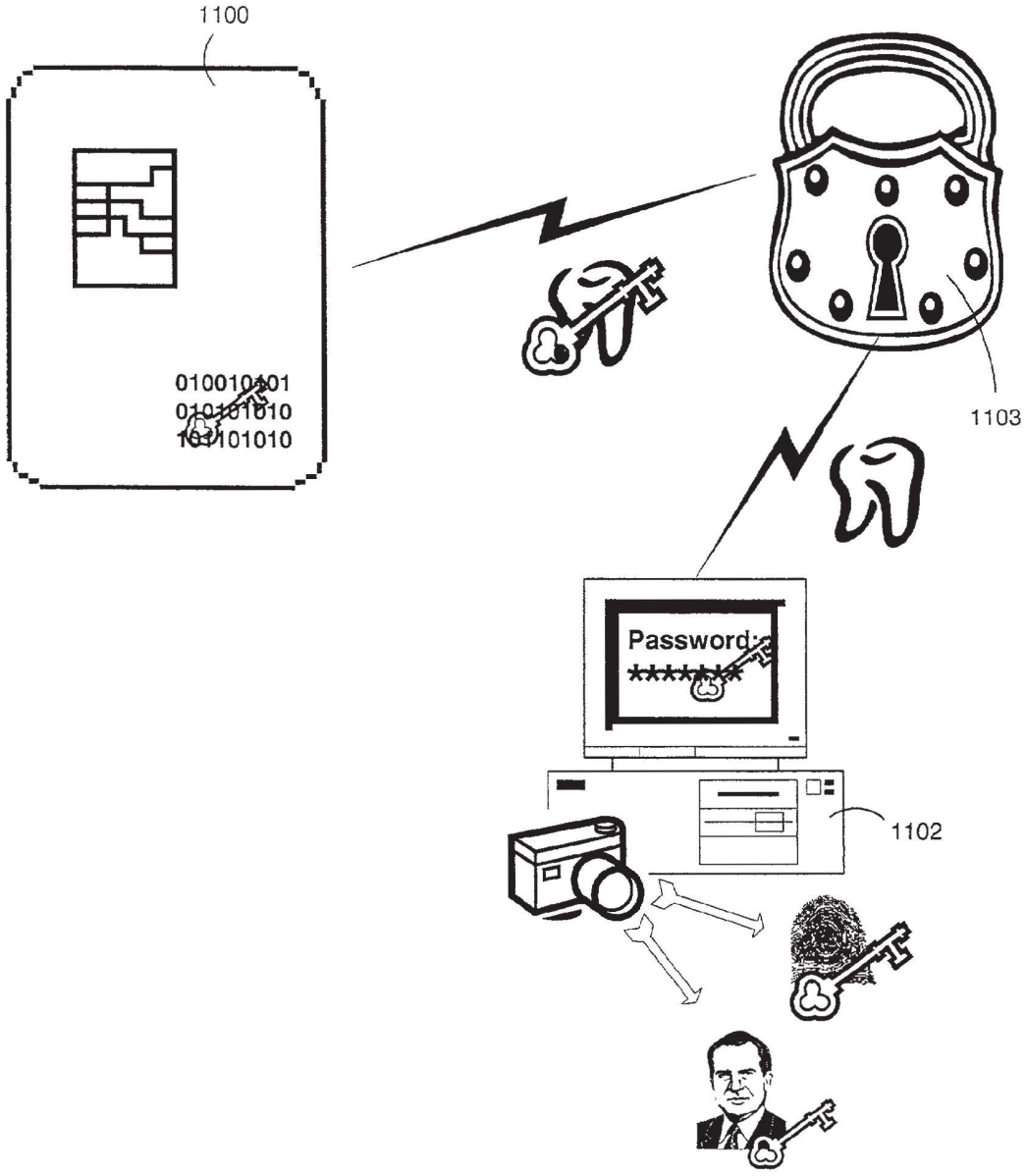


FIG. 11B

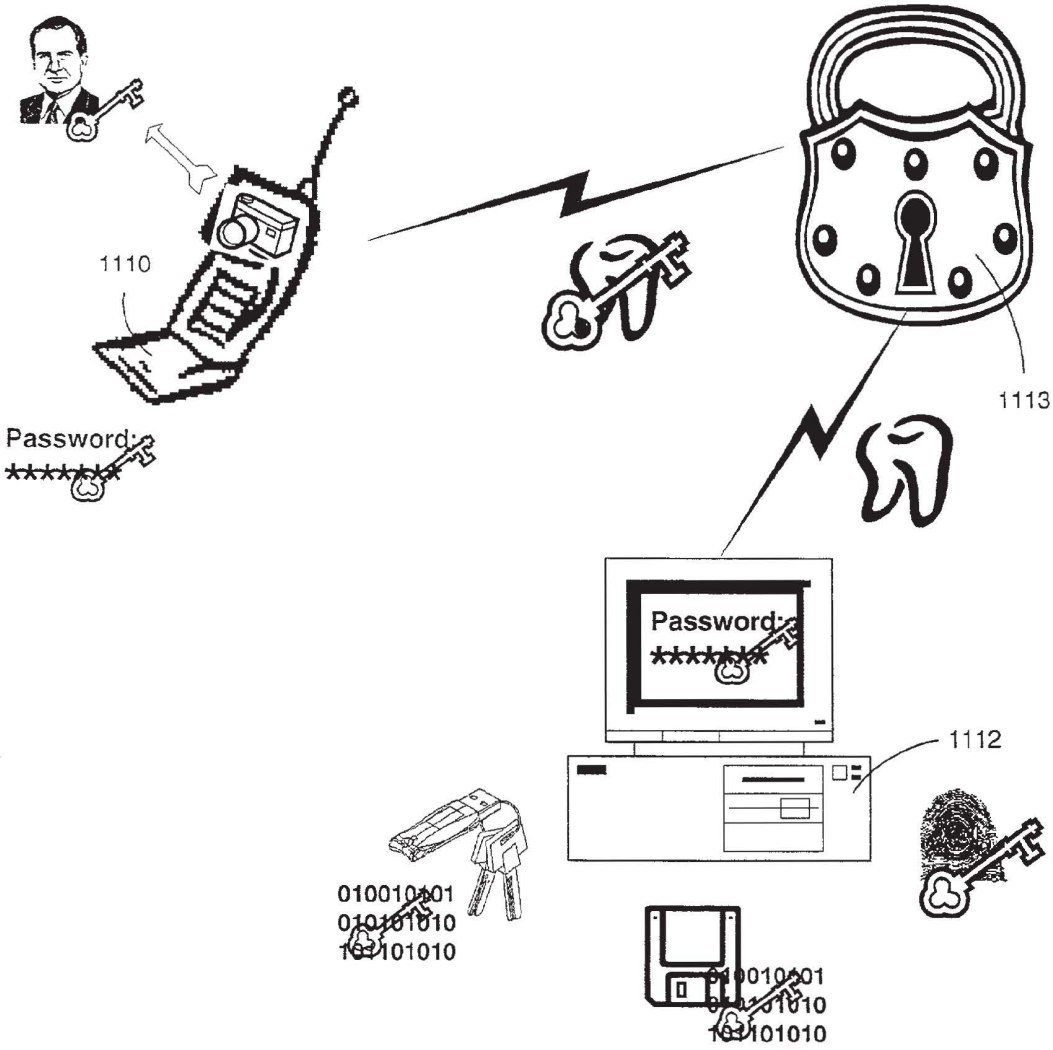

1110
Password:
****
1113
Password:
****
1112
010010101
010101010
101101010
010010101
010101010
101101010

FIG. 11C

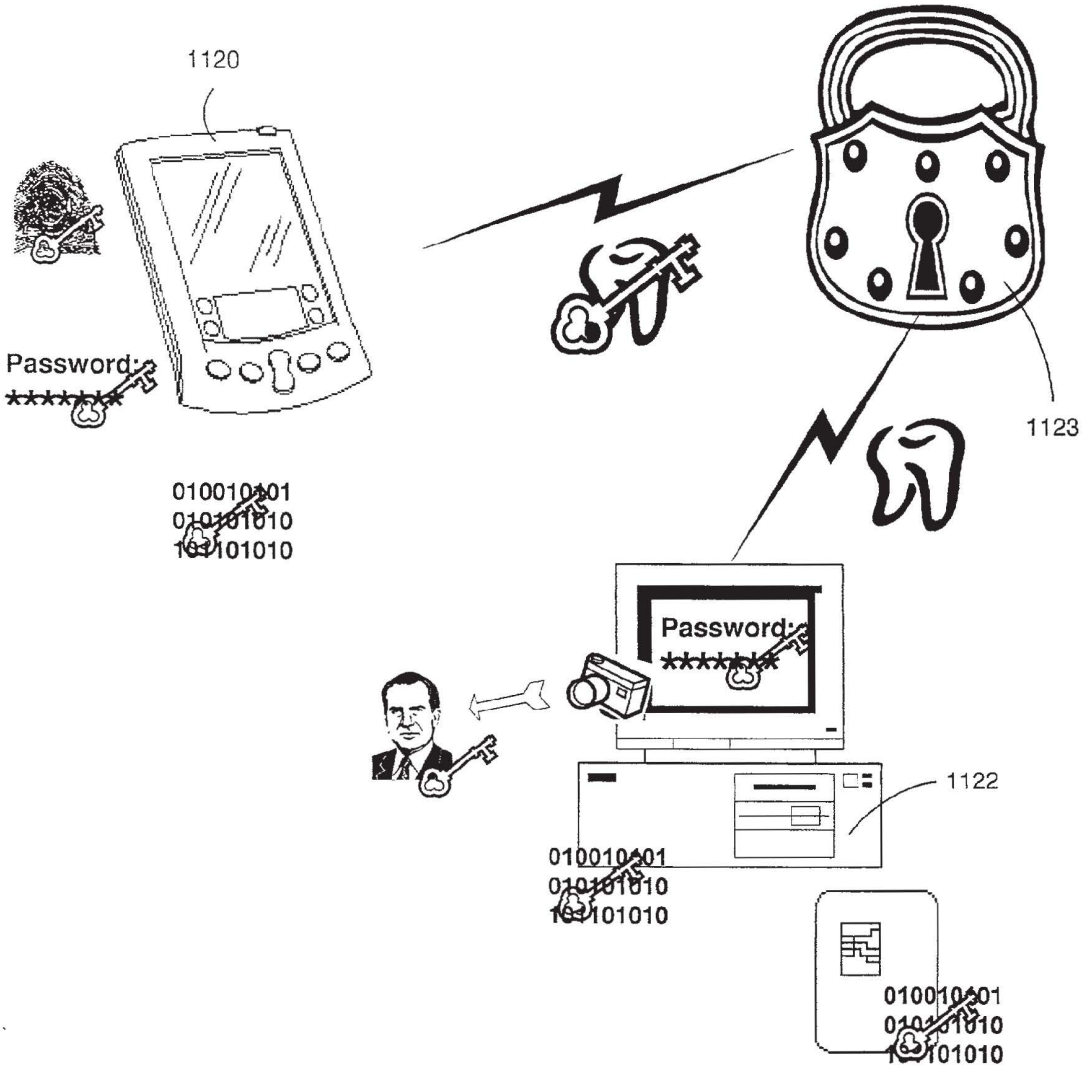

1120
Password:
****
010010101
010101010
101101010
1123
Password:
****
1122
010010101
010101010
101101010
010010101
010101010
101101010

FIG. 11D

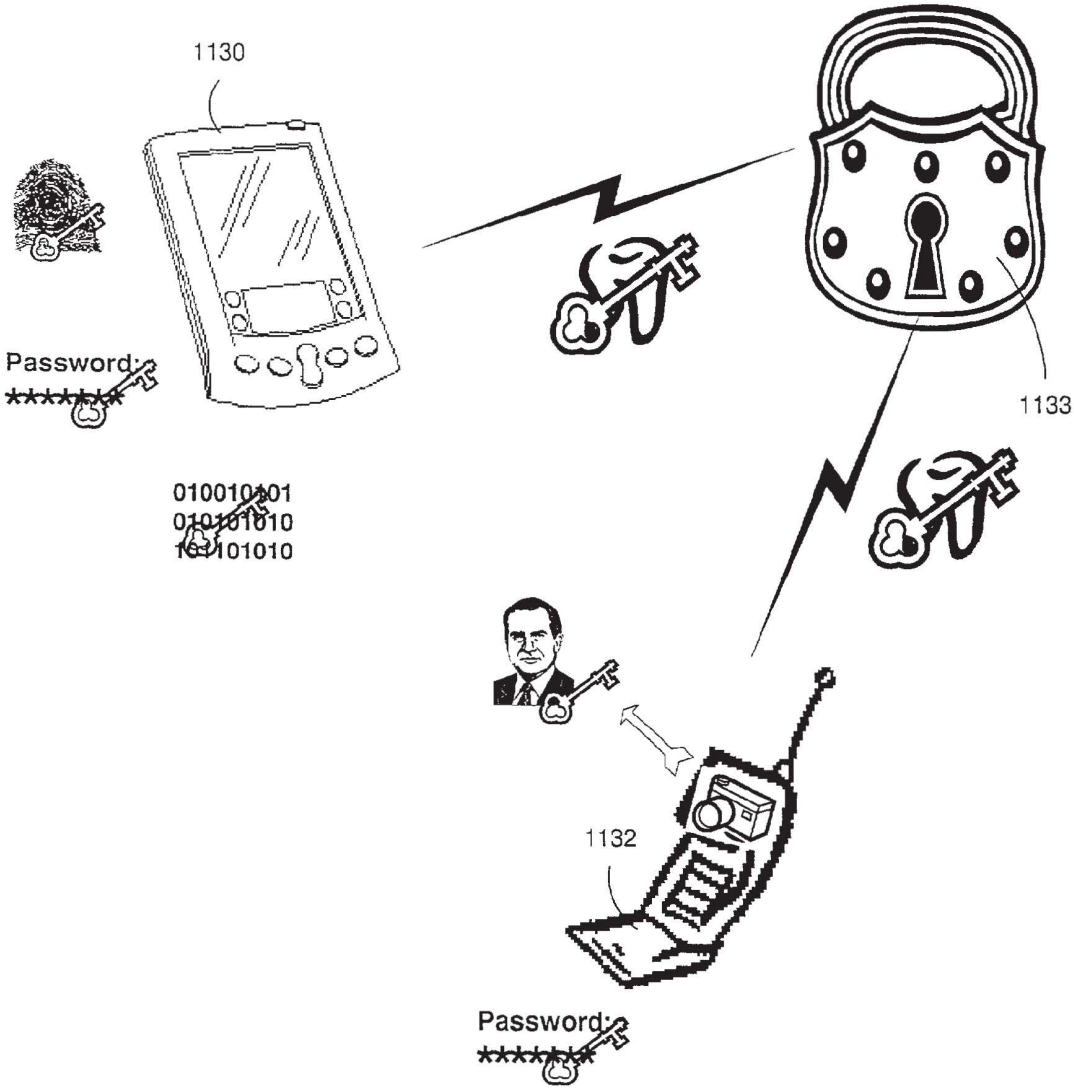

1130
Password:
****
010010101
010101010
1010101010
1133
1132
Password:
****

FIG. 11E

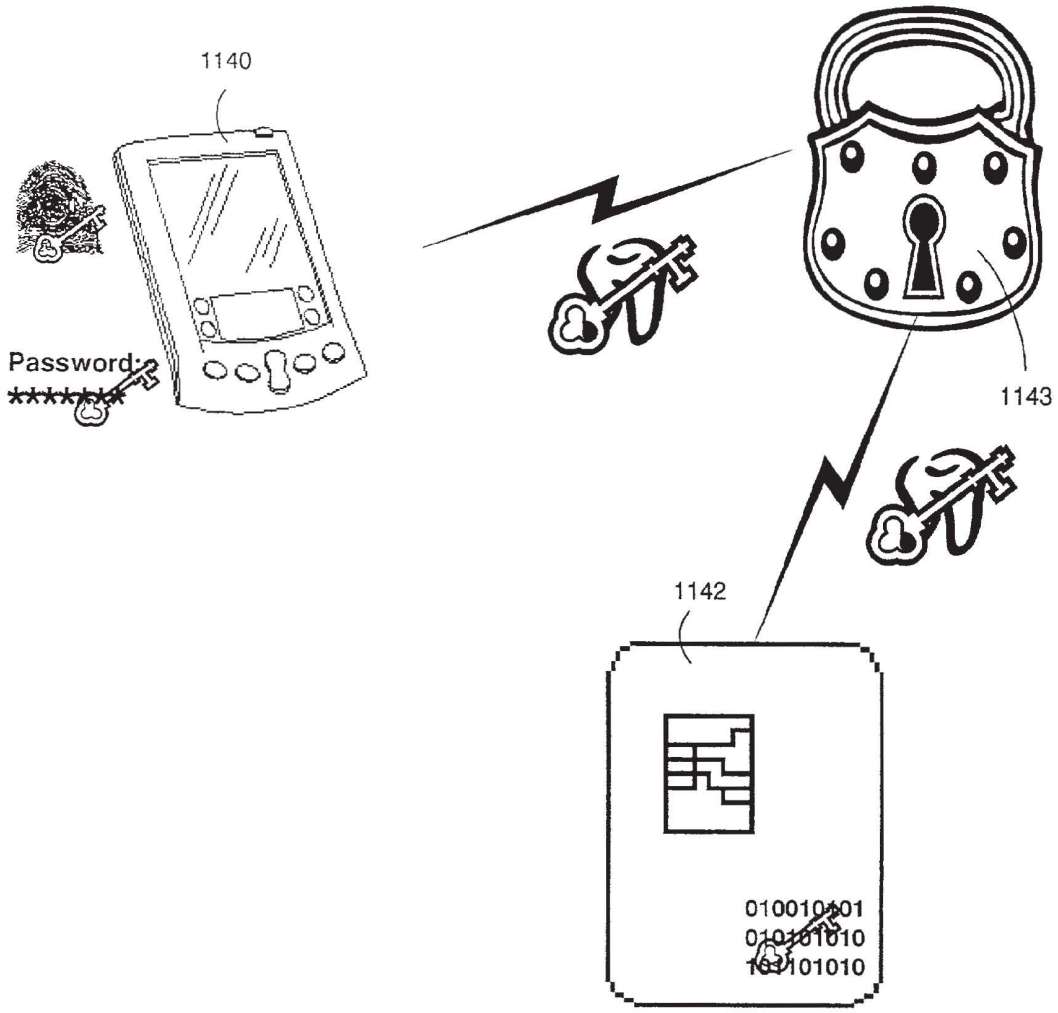


FIG. 11F

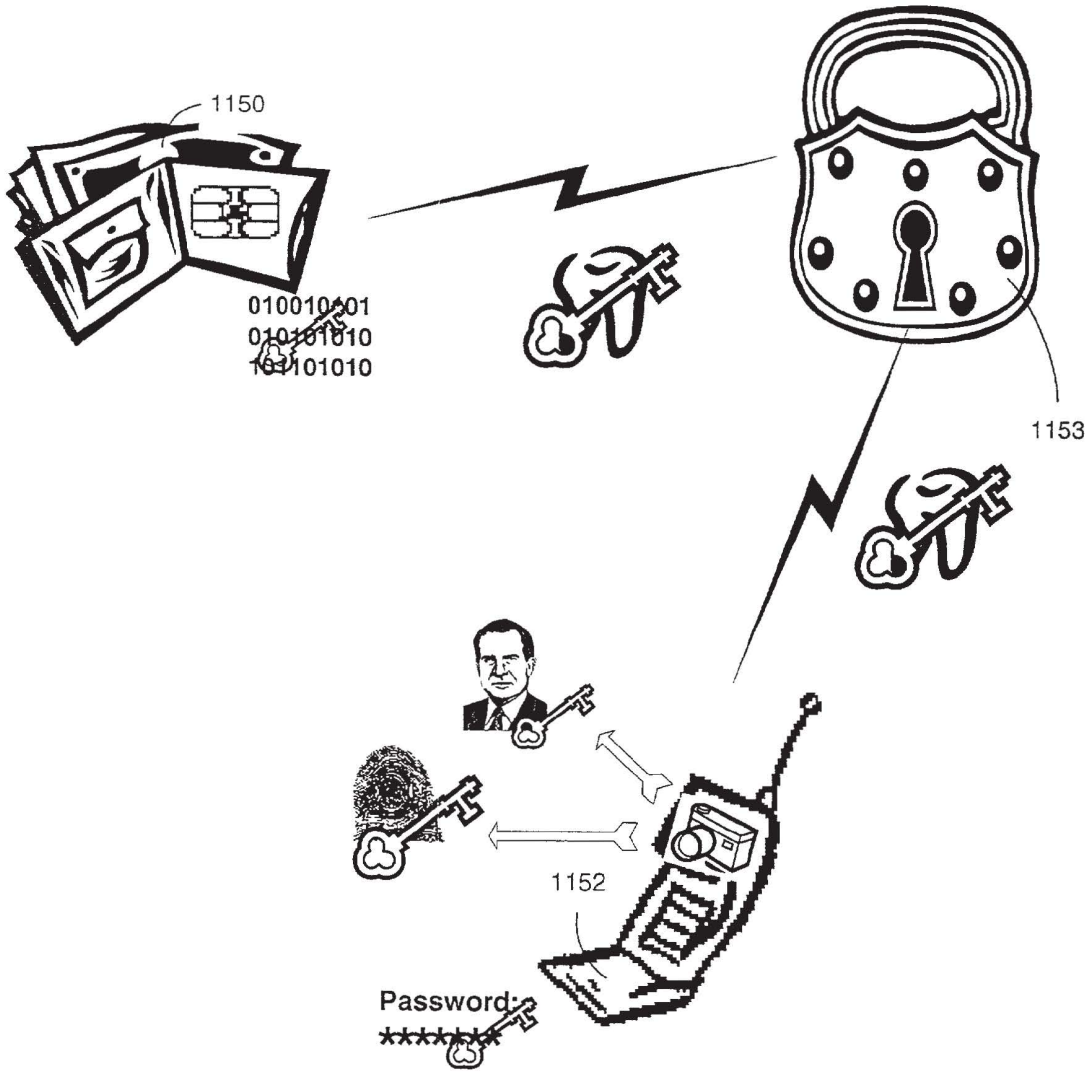


FIG. 12A

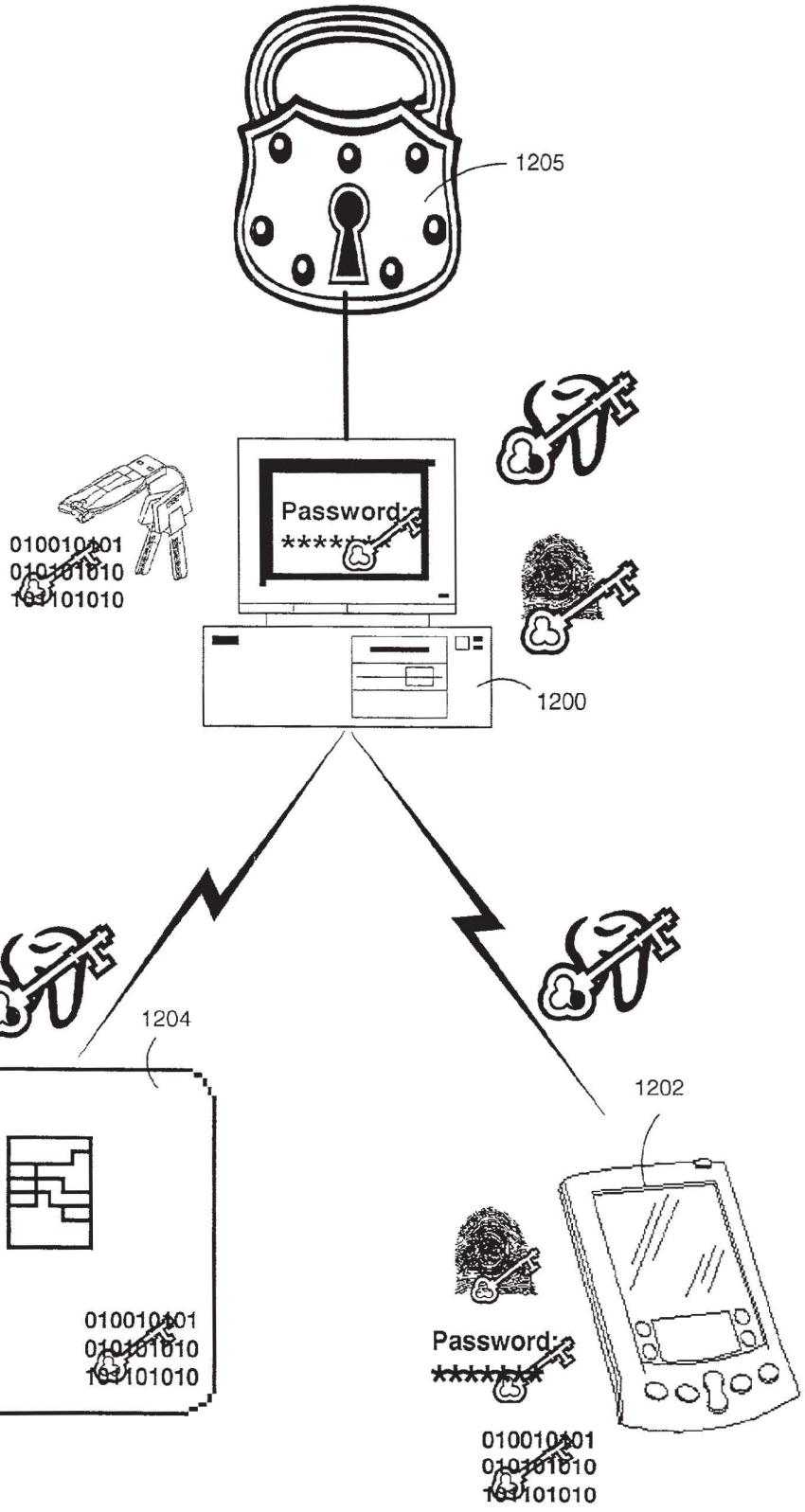


FIG. 12B

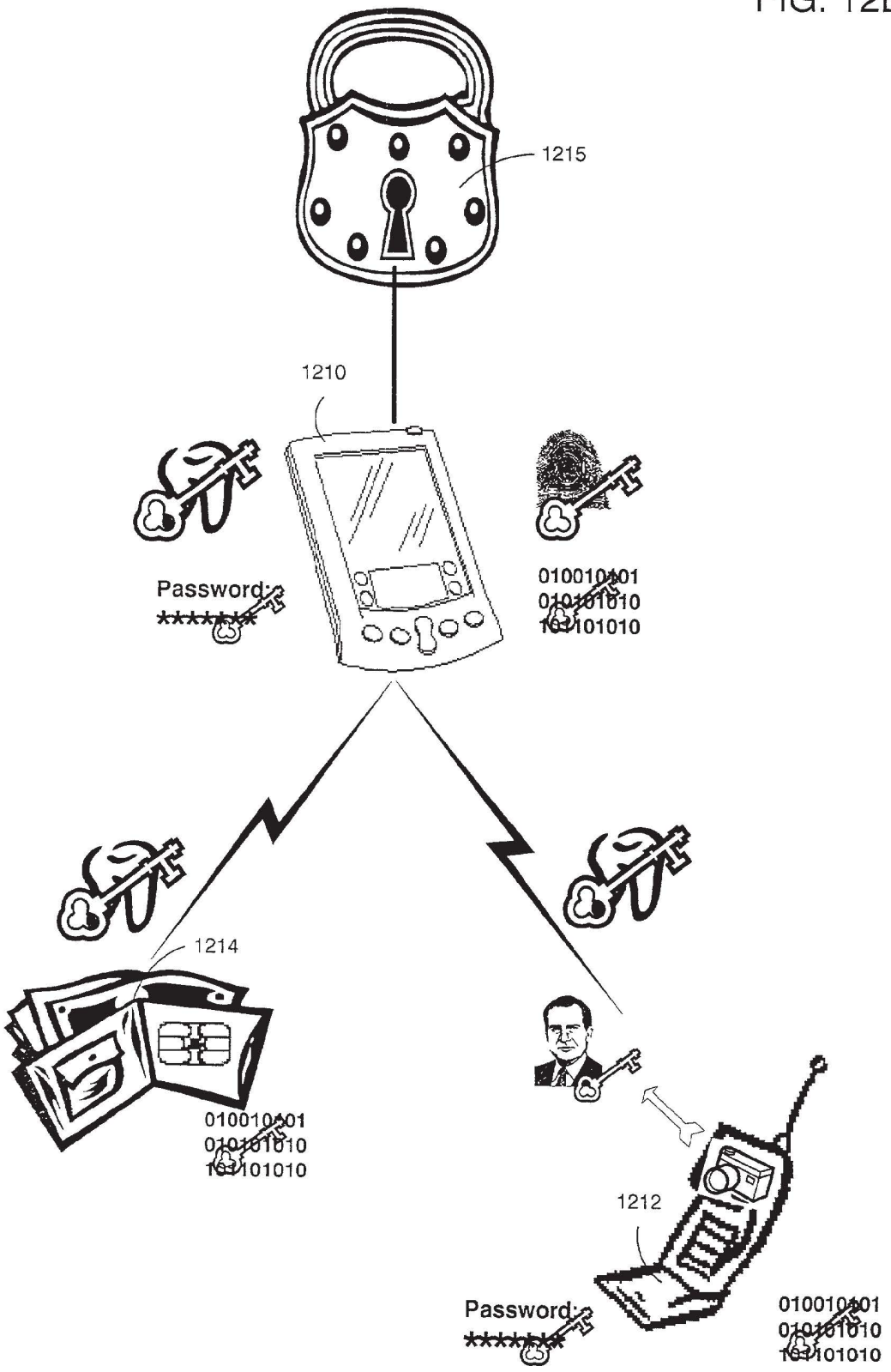

1215
1210
Password:
****
010010101
010101010
101101010
1214
010010101
010101010
101101010
1212
Password:
****
010010101
010101010
101101010

FIG. 12C

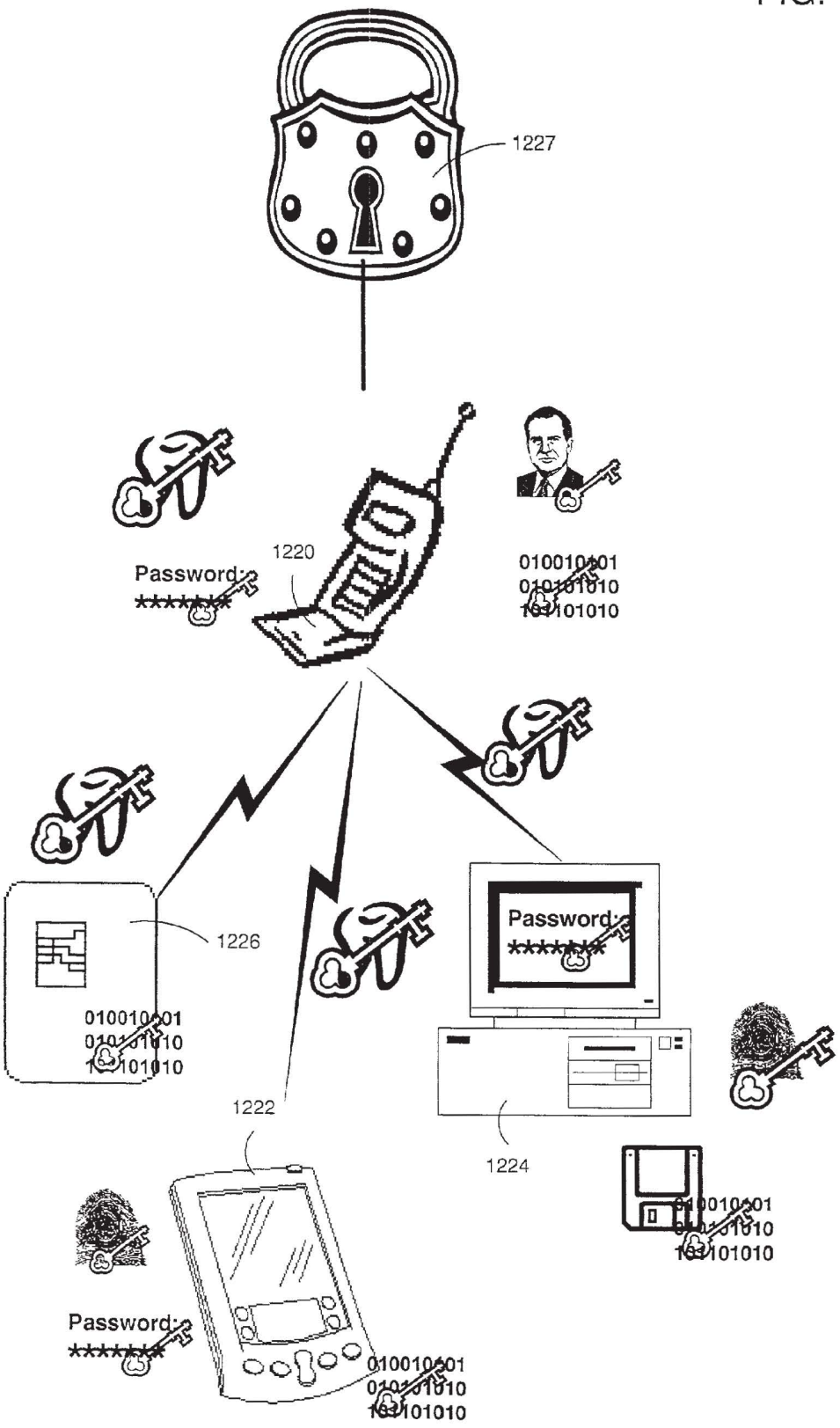

1227
1220
Password:
****
010010101
1226
Password:
****
1222
1224
Password:
****

FIG. 13A

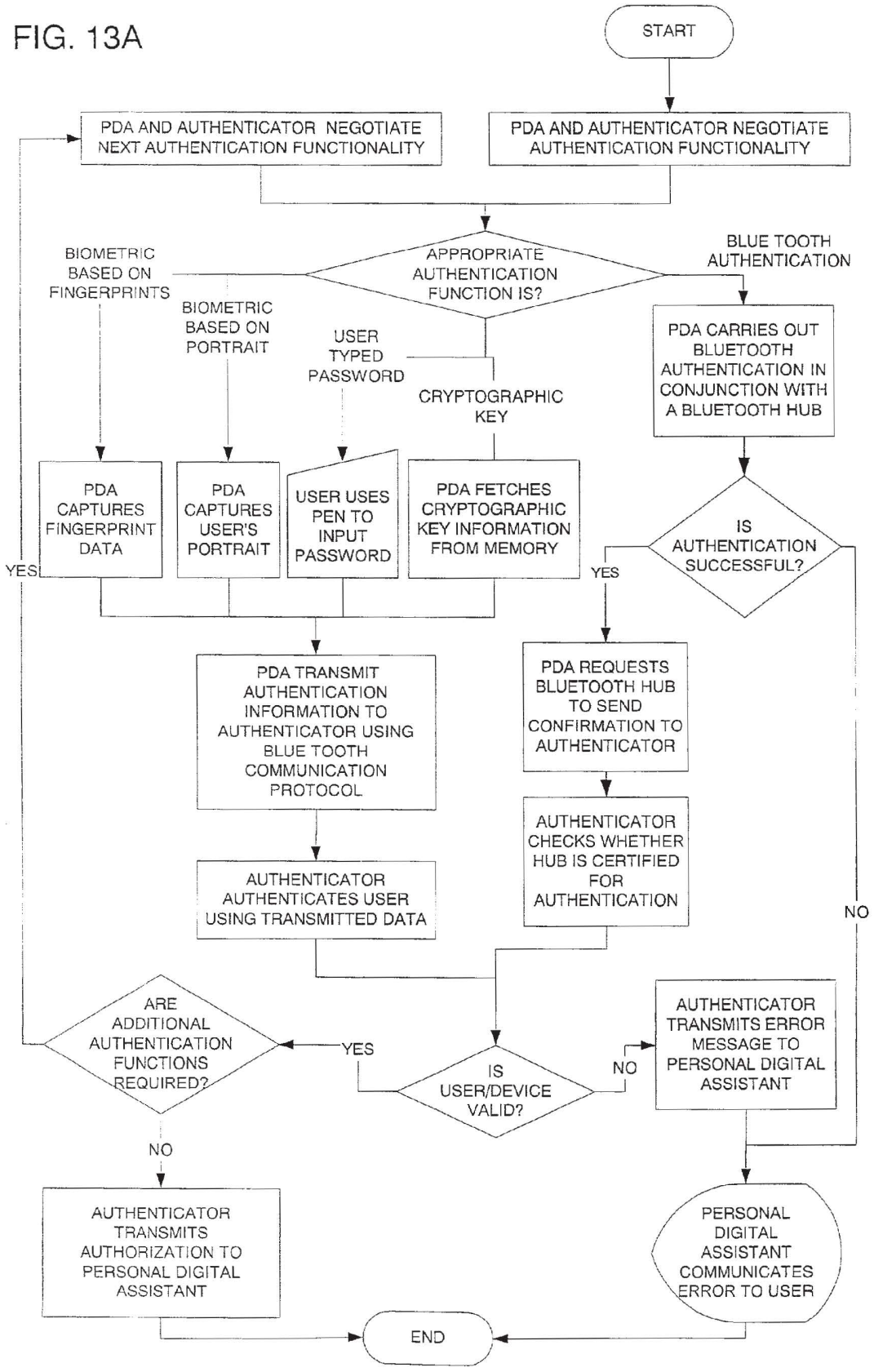

START
PDA AND AUTHENTICATOR NEGOTIATE NEXT AUTHENTICATION FUNCTIONALITY
PDA AND AUTHENTICATOR NEGOTIATE AUTHENTICATION FUNCTIONALITY
APPROPRIATE AUTHENTICATION FUNCTION IS?
BIOMETRIC BASED ON FINGERPRINTS
BIOMETRIC BASED ON PORTRAIT
USER TYPED PASSWORD
CRYPTOGRAPHIC KEY
BLUE TOOTH AUTHENTICATION
PDA CAPTURES FINGERPRINT DATA
PDA CAPTURES USER'S PORTRAIT
USER USES PEN TO INPUT PASSWORD
PDA FETCHES CRYPTOGRAPHIC KEY INFORMATION FROM MEMORY
PDA CARRIES OUT BLUETOOTH AUTHENTICATION IN CONJUNCTION WITH A BLUETOOTH HUB
IS AUTHENTICATION SUCCESSFUL?
YES
NO
PDA TRANSMIT AUTHENTICATION INFORMATION TO AUTHENTICATOR USING BLUE TOOTH COMMUNICATION PROTOCOL
PDA REQUESTS BLUETOOTH HUB TO SEND CONFIRMATION TO AUTHENTICATOR
AUTHENTICATOR CHECKS WHETHER HUB IS CERTIFIED FOR AUTHENTICATION
AUTHENTICATOR AUTHENTICATES USER USING TRANSMITTED DATA
ARE ADDITIONAL AUTHENTICATION FUNCTIONS REQUIRED?
IS USER/DEVICE VALID?
AUTHENTICATOR TRANSMITS ERROR MESSAGE TO PERSONAL DIGITAL ASSISTANT
AUTHENTICATOR TRANSMITS AUTHORIZATION TO PERSONAL DIGITAL ASSISTANT
PERSONAL DIGITAL ASSISTANT COMMUNICATES ERROR TO USER
END

FIG. 13B

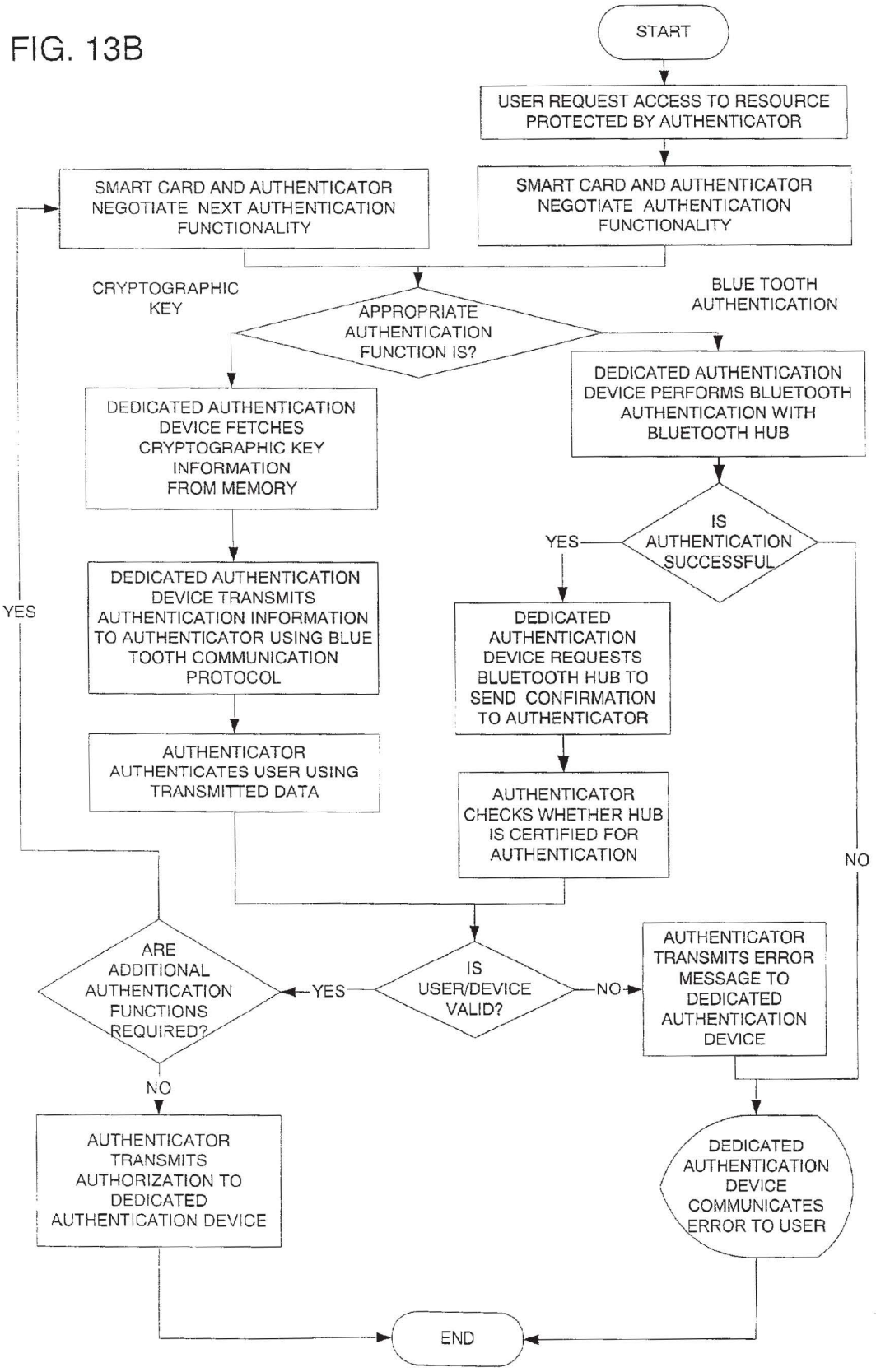

START
USER REQUEST ACCESS TO RESOURCE PROTECTED BY AUTHENTICATOR
SMART CARD AND AUTHENTICATOR NEGOTIATE AUTHENTICATION FUNCTIONALITY
SMART CARD AND AUTHENTICATOR NEGOTIATE NEXT AUTHENTICATION FUNCTIONALITY
CRYPTOGRAPHIC KEY
APPROPRIATE AUTHENTICATION FUNCTION IS?
BLUE TOOTH AUTHENTICATION
DEDICATED AUTHENTICATION DEVICE FETCHES CRYPTOGRAPHIC KEY INFORMATION FROM MEMORY
DEDICATED AUTHENTICATION DEVICE PERFORMS BLUETOOTH AUTHENTICATION WITH BLUETOOTH HUB
IS AUTHENTICATION SUCCESSFUL
YES
NO
DEDICATED AUTHENTICATION DEVICE TRANSMITS AUTHENTICATION INFORMATION TO AUTHENTICATOR USING BLUE TOOTH COMMUNICATION PROTOCOL
DEDICATED AUTHENTICATION DEVICE REQUESTS BLUETOOTH HUB TO SEND CONFIRMATION TO AUTHENTICATOR
AUTHENTICATOR AUTHENTICATES USER USING TRANSMITTED DATA
AUTHENTICATOR CHECKS WHETHER HUB IS CERTIFIED FOR AUTHENTICATION
ARE ADDITIONAL AUTHENTICATION FUNCTIONS REQUIRED?
IS USER/DEVICE VALID?
AUTHENTICATOR TRANSMITS ERROR MESSAGE TO DEDICATED AUTHENTICATION DEVICE
AUTHENTICATOR TRANSMITS AUTHORIZATION TO DEDICATED AUTHENTICATION DEVICE
DEDICATED AUTHENTICATION DEVICE COMMUNICATES ERROR TO USER
END

FIG. 13C

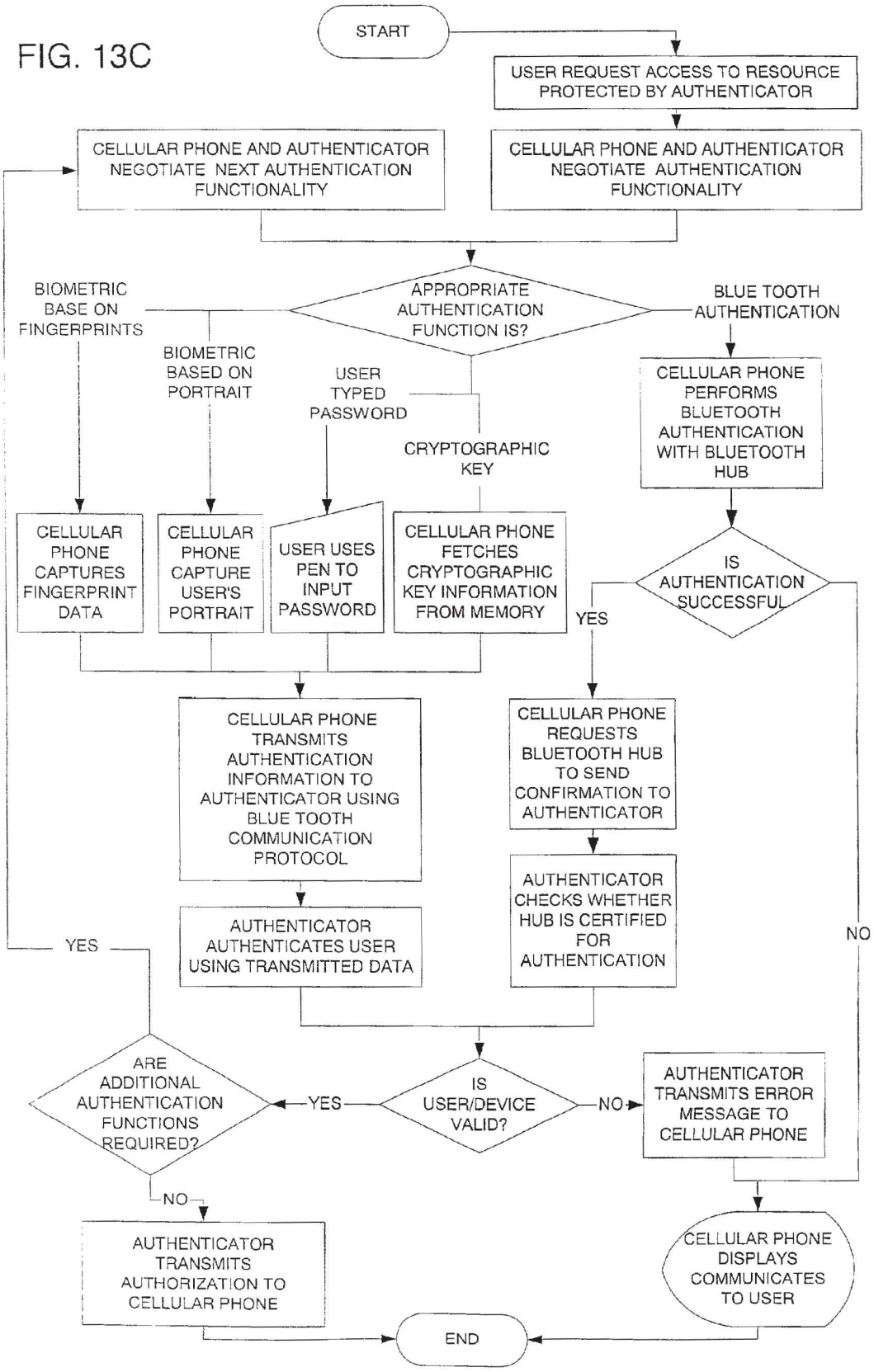

START
USER REQUEST ACCESS TO RESOURCE PROTECTED BY AUTHENTICATOR
CELLULAR PHONE AND AUTHENTICATOR NEGOTIATE AUTHENTICATION FUNCTIONALITY
CELLULAR PHONE AND AUTHENTICATOR NEGOTIATE NEXT AUTHENTICATION FUNCTIONALITY
APPROPRIATE AUTHENTICATION FUNCTION IS?
BIOMETRIC BASE ON FINGERPRINTS
BIOMETRIC BASED ON PORTRAIT
USER TYPED PASSWORD
CRYPTOGRAPHIC KEY
BLUE TOOTH AUTHENTICATION
CELLULAR PHONE CAPTURES FINGERPRINT DATA
CELLULAR PHONE CAPTURE USER'S PORTRAIT
USER USES PEN TO INPUT PASSWORD
CELLULAR PHONE FETCHES CRYPTOGRAPHIC KEY INFORMATION FROM MEMORY
CELLULAR PHONE PERFORMS BLUETOOTH AUTHENTICATION WITH BLUETOOTH HUB
IS AUTHENTICATION SUCCESSFUL
YES
NO
CELLULAR PHONE TRANSMITS AUTHENTICATION INFORMATION TO AUTHENTICATOR USING BLUE TOOTH COMMUNICATION PROTOCOL
CELLULAR PHONE REQUESTS BLUETOOTH HUB TO SEND CONFIRMATION TO AUTHENTICATOR
AUTHENTICATOR AUTHENTICATES USER USING TRANSMITTED DATA
AUTHENTICATOR CHECKS WHETHER HUB IS CERTIFIED FOR AUTHENTICATION
YES
ARE ADDITIONAL AUTHENTICATION FUNCTIONS REQUIRED?
YES
IS USER/DEVICE VALID?
NO
AUTHENTICATOR TRANSMITS ERROR MESSAGE TO CELLULAR PHONE
NO
AUTHENTICATOR TRANSMITS AUTHORIZATION TO CELLULAR PHONE
CELLULAR PHONE DISPLAYS COMMUNICATES TO USER
END

FIG. 13D

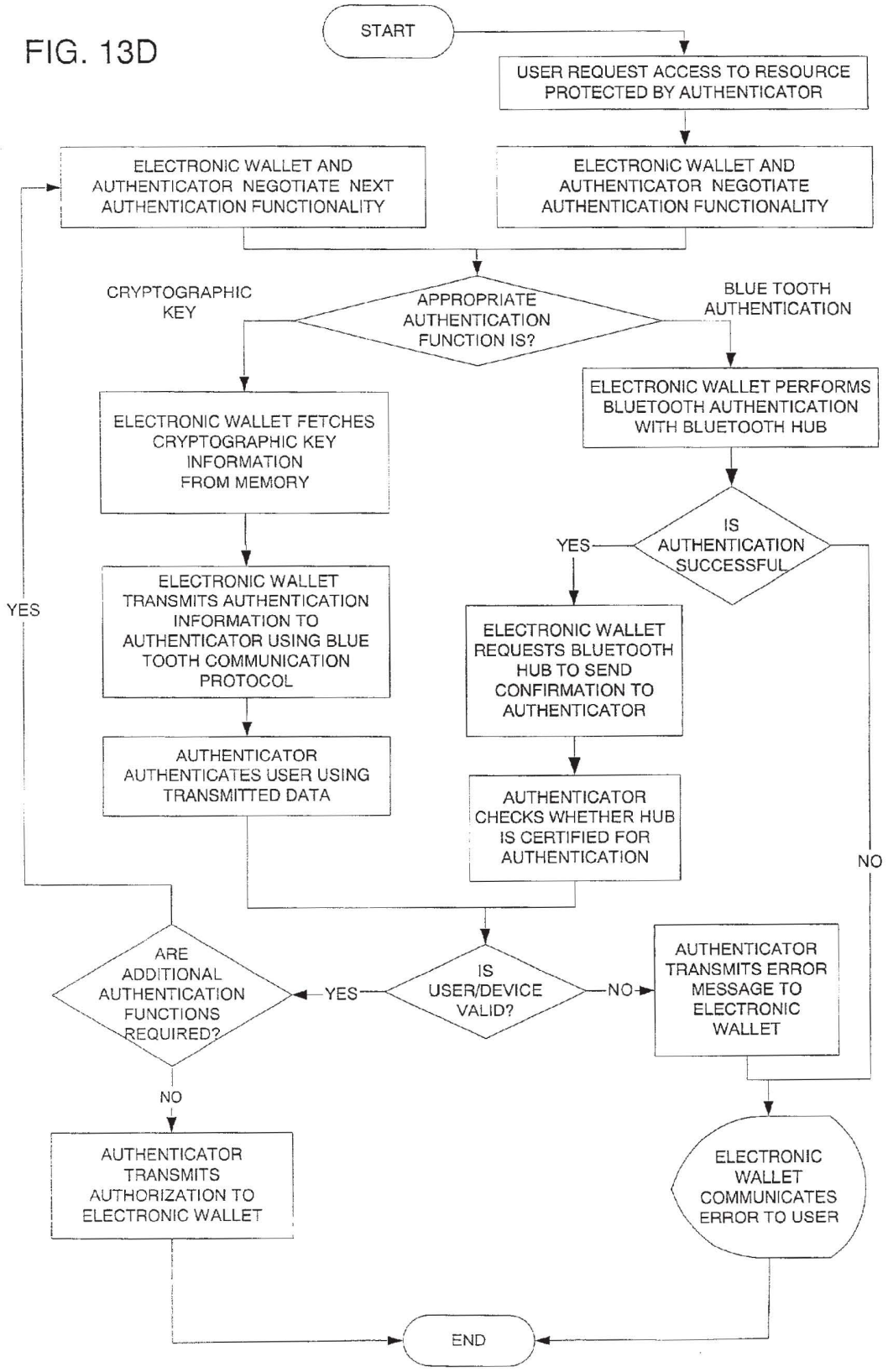

START
USER REQUEST ACCESS TO RESOURCE PROTECTED BY AUTHENTICATOR
ELECTRONIC WALLET AND AUTHENTICATOR NEGOTIATE NEXT AUTHENTICATION FUNCTIONALITY
ELECTRONIC WALLET AND AUTHENTICATOR NEGOTIATE AUTHENTICATION FUNCTIONALITY
CRYPTOGRAPHIC KEY
APPROPRIATE AUTHENTICATION FUNCTION IS?
BLUE TOOTH AUTHENTICATION
ELECTRONIC WALLET FETCHES CRYPTOGRAPHIC KEY INFORMATION FROM MEMORY
ELECTRONIC WALLET PERFORMS BLUETOOTH AUTHENTICATION WITH BLUETOOTH HUB
IS AUTHENTICATION SUCCESSFUL
YES
NO
ELECTRONIC WALLET TRANSMITS AUTHENTICATION INFORMATION TO AUTHENTICATOR USING BLUE TOOTH COMMUNICATION PROTOCOL
ELECTRONIC WALLET REQUESTS BLUETOOTH HUB TO SEND CONFIRMATION TO AUTHENTICATOR
AUTHENTICATOR AUTHENTICATES USER USING TRANSMITTED DATA
AUTHENTICATOR CHECKS WHETHER HUB IS CERTIFIED FOR AUTHENTICATION
ARE ADDITIONAL AUTHENTICATION FUNCTIONS REQUIRED?
YES
IS USER/DEVICE VALID?
NO
AUTHENTICATOR TRANSMITS ERROR MESSAGE TO ELECTRONIC WALLET
NO
AUTHENTICATOR TRANSMITS AUTHORIZATION TO ELECTRONIC WALLET
ELECTRONIC WALLET COMMUNICATES ERROR TO USER
END

FIG. 13E

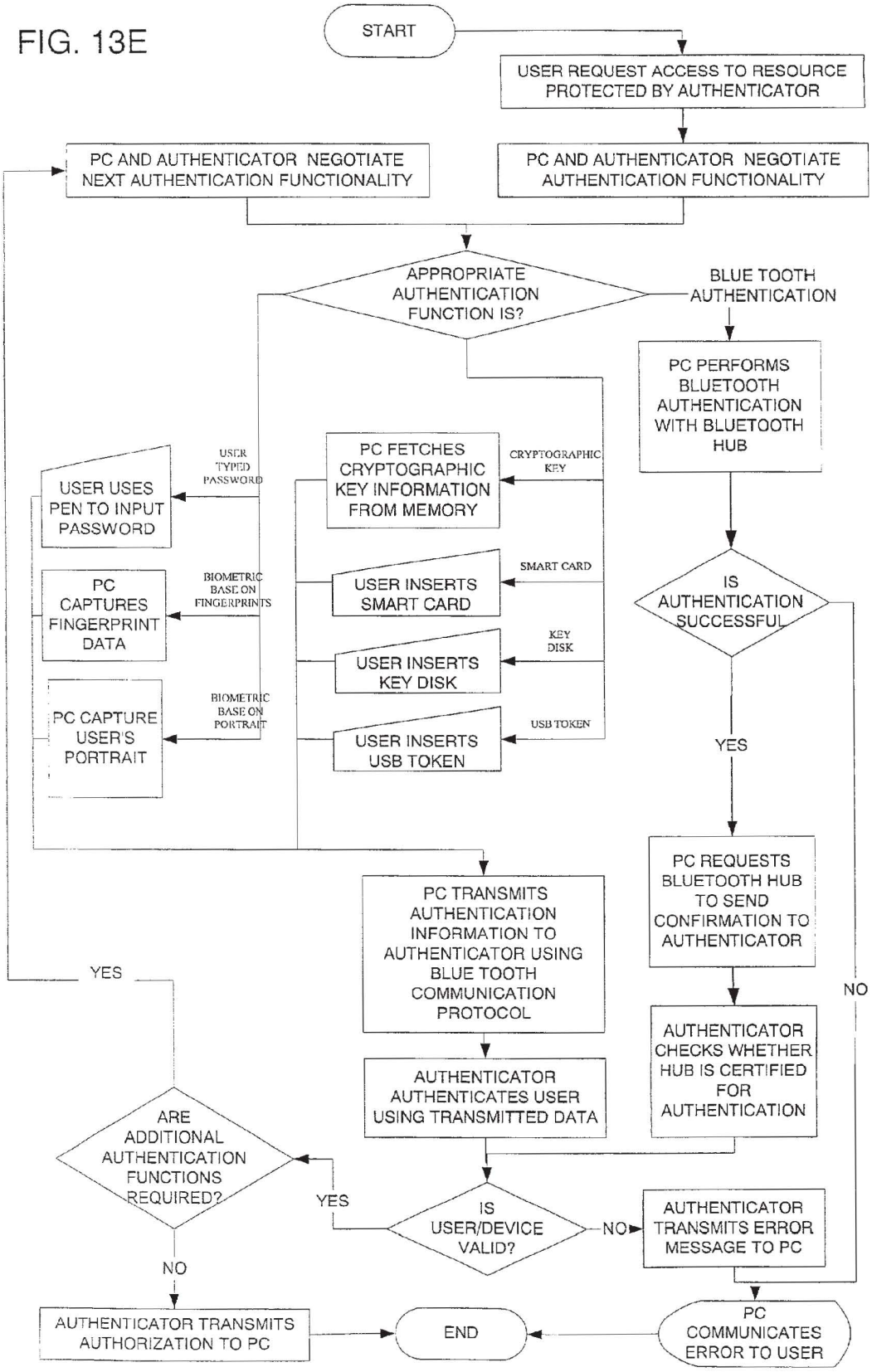

START
USER REQUEST ACCESS TO RESOURCE PROTECTED BY AUTHENTICATOR
PC AND AUTHENTICATOR NEGOTIATE AUTHENTICATION FUNCTIONALITY
PC AND AUTHENTICATOR NEGOTIATE NEXT AUTHENTICATION FUNCTIONALITY
APPROPRIATE AUTHENTICATION FUNCTION IS?
BLUE TOOTH AUTHENTICATION
PC PERFORMS BLUETOOTH AUTHENTICATION WITH BLUETOOTH HUB
IS AUTHENTICATION SUCCESSFUL
YES
NO
PC FETCHES CRYPTOGRAPHIC KEY INFORMATION FROM MEMORY
CRYPTOGRAPHIC KEY
USER USES PEN TO INPUT PASSWORD
USER TYPED PASSWORD
USER INSERTS SMART CARD
SMART CARD
PC CAPTURES FINGERPRINT DATA
BIOMETRIC BASE ON FINGERPRINTS
USER INSERTS KEY DISK
KEY DISK
PC CAPTURE USER'S PORTRAIT
BIOMETRIC BASE ON PORTRAIT
USER INSERTS USB TOKEN
USB TOKEN
PC TRANSMITS AUTHENTICATION INFORMATION TO AUTHENTICATOR USING BLUE TOOTH COMMUNICATION PROTOCOL
PC REQUESTS BLUETOOTH HUB TO SEND CONFIRMATION TO AUTHENTICATOR
AUTHENTICATOR CHECKS WHETHER HUB IS CERTIFIED FOR AUTHENTICATION
AUTHENTICATOR AUTHENTICATES USER USING TRANSMITTED DATA
ARE ADDITIONAL AUTHENTICATION FUNCTIONS REQUIRED?
YES
NO
IS USER/DEVICE VALID?
YES
NO
AUTHENTICATOR TRANSMITS ERROR MESSAGE TO PC
AUTHENTICATOR TRANSMITS AUTHORIZATION TO PC
END
PC COMMUNICATES ERROR TO USER

FIG. 14A

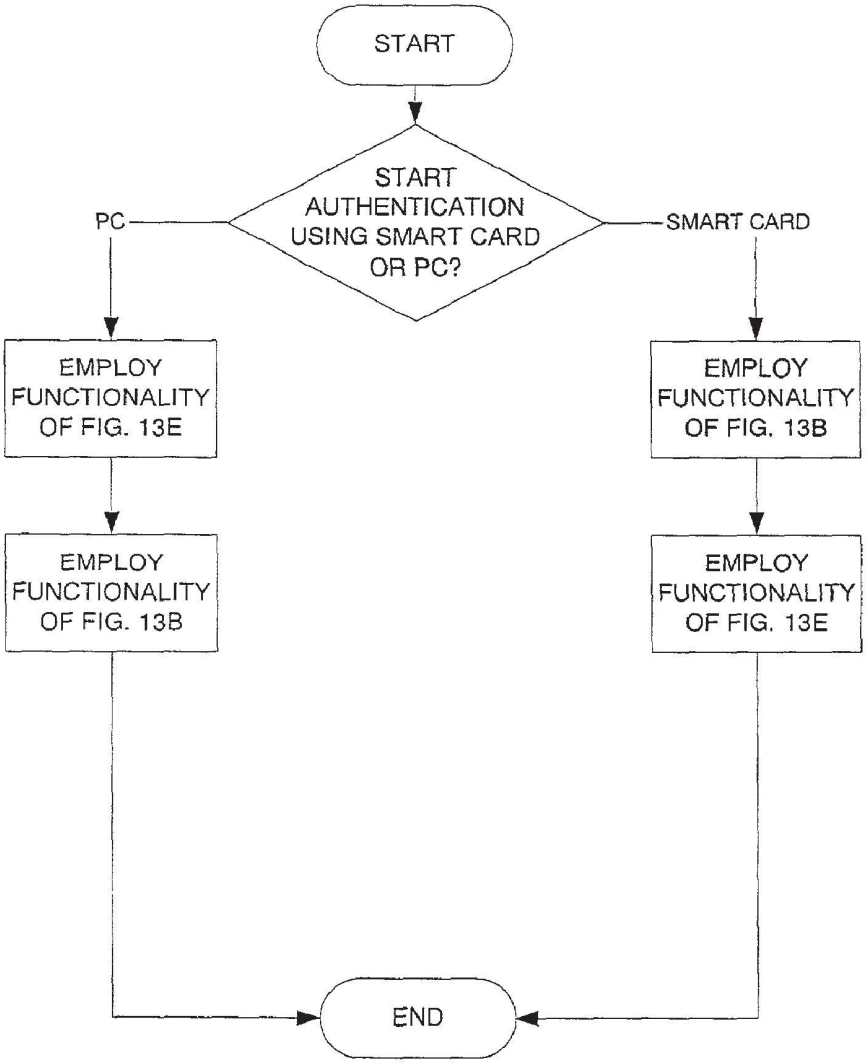

START
START AUTHENTICATION USING SMART CARD OR PC?
PC
SMART CARD
EMPLOY FUNCTIONALITY OF FIG. 13E
EMPLOY FUNCTIONALITY OF FIG. 13B
EMPLOY FUNCTIONALITY OF FIG. 13B
EMPLOY FUNCTIONALITY OF FIG. 13E
END

FIG. 14B

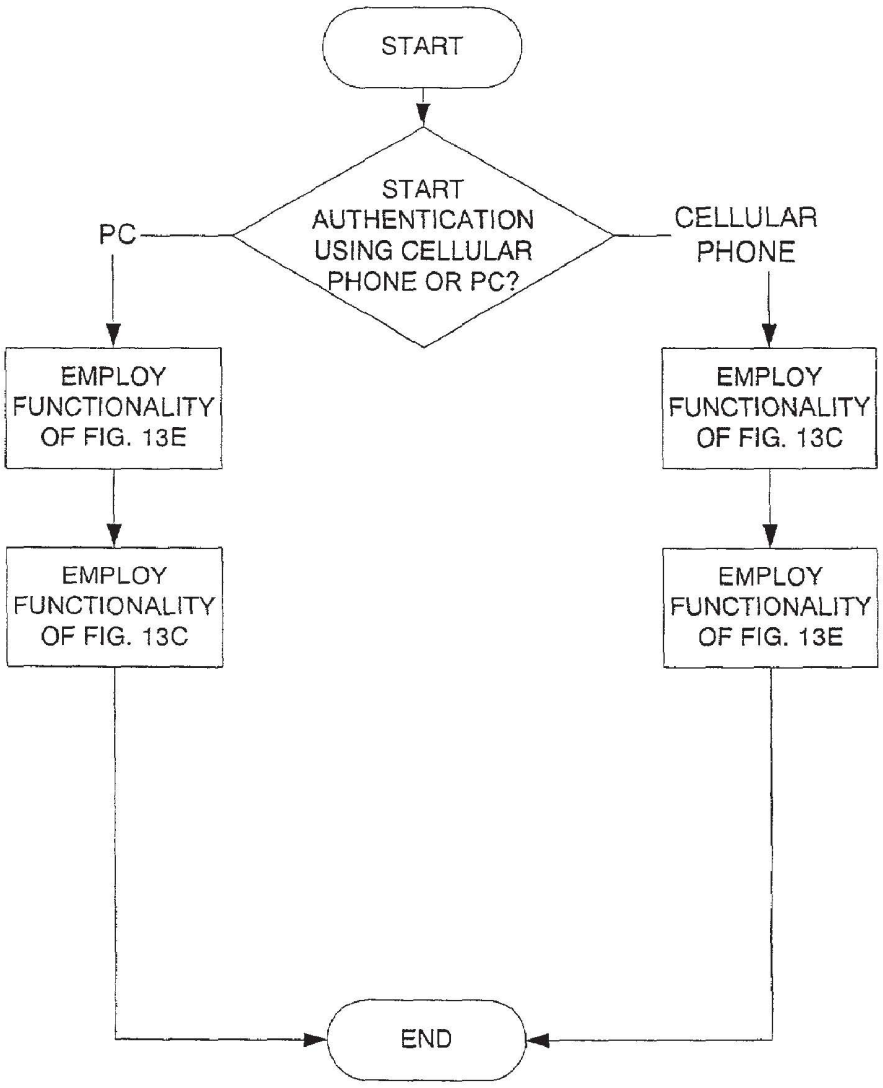

START
START AUTHENTICATION USING CELLULAR PHONE OR PC?
PC
CELLULAR PHONE
EMPLOY FUNCTIONALITY OF FIG. 13E
EMPLOY FUNCTIONALITY OF FIG. 13C
EMPLOY FUNCTIONALITY OF FIG. 13C
EMPLOY FUNCTIONALITY OF FIG. 13E
END

FIG. 14C

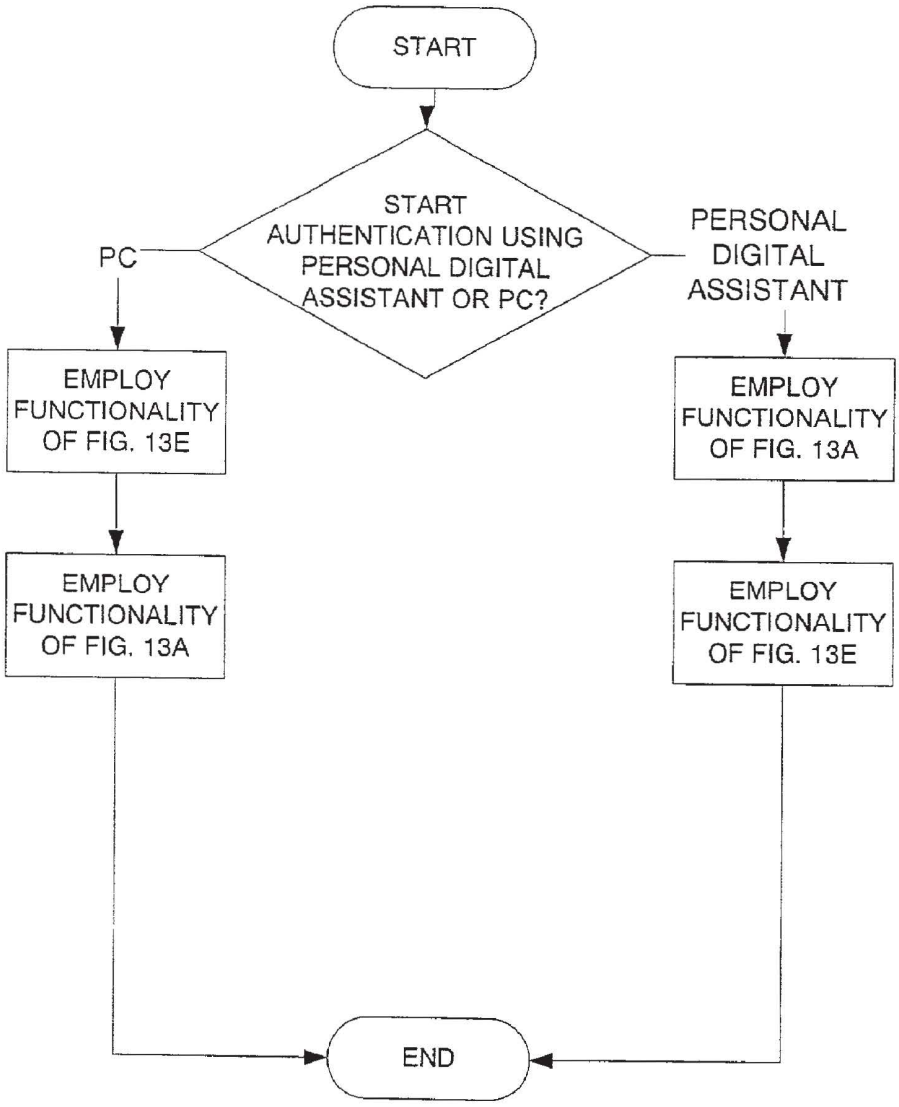

START
START AUTHENTICATION USING PERSONAL DIGITAL ASSISTANT OR PC?
PC
PERSONAL DIGITAL ASSISTANT
EMPLOY FUNCTIONALITY OF FIG. 13E
EMPLOY FUNCTIONALITY OF FIG. 13A
EMPLOY FUNCTIONALITY OF FIG. 13A
EMPLOY FUNCTIONALITY OF FIG. 13E
END

FIG. 14D

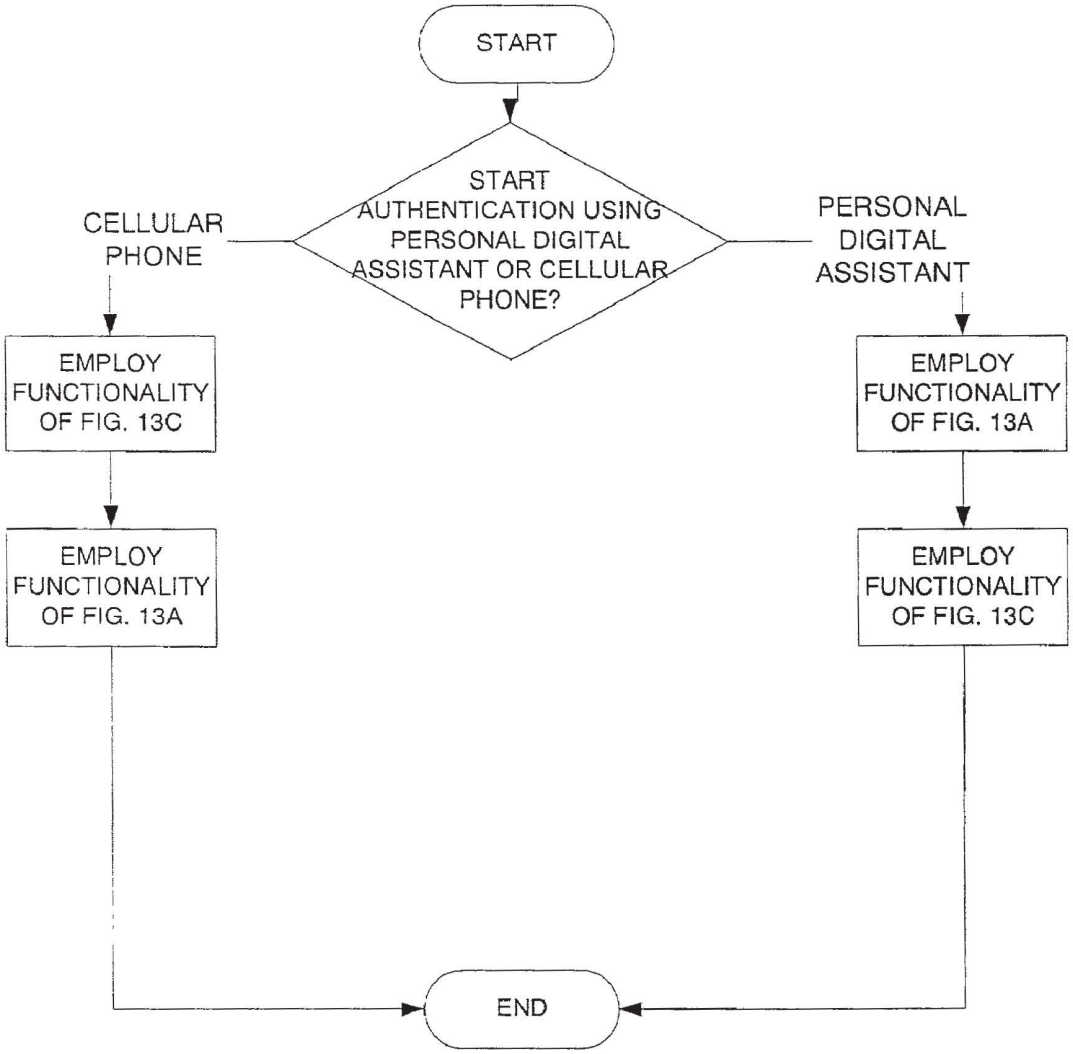

START
START AUTHENTICATION USING PERSONAL DIGITAL ASSISTANT OR CELLULAR PHONE?
CELLULAR PHONE
PERSONAL DIGITAL ASSISTANT
EMPLOY FUNCTIONALITY OF FIG. 13C
EMPLOY FUNCTIONALITY OF FIG. 13A
EMPLOY FUNCTIONALITY OF FIG. 13A
EMPLOY FUNCTIONALITY OF FIG. 13C
END

FIG. 14E

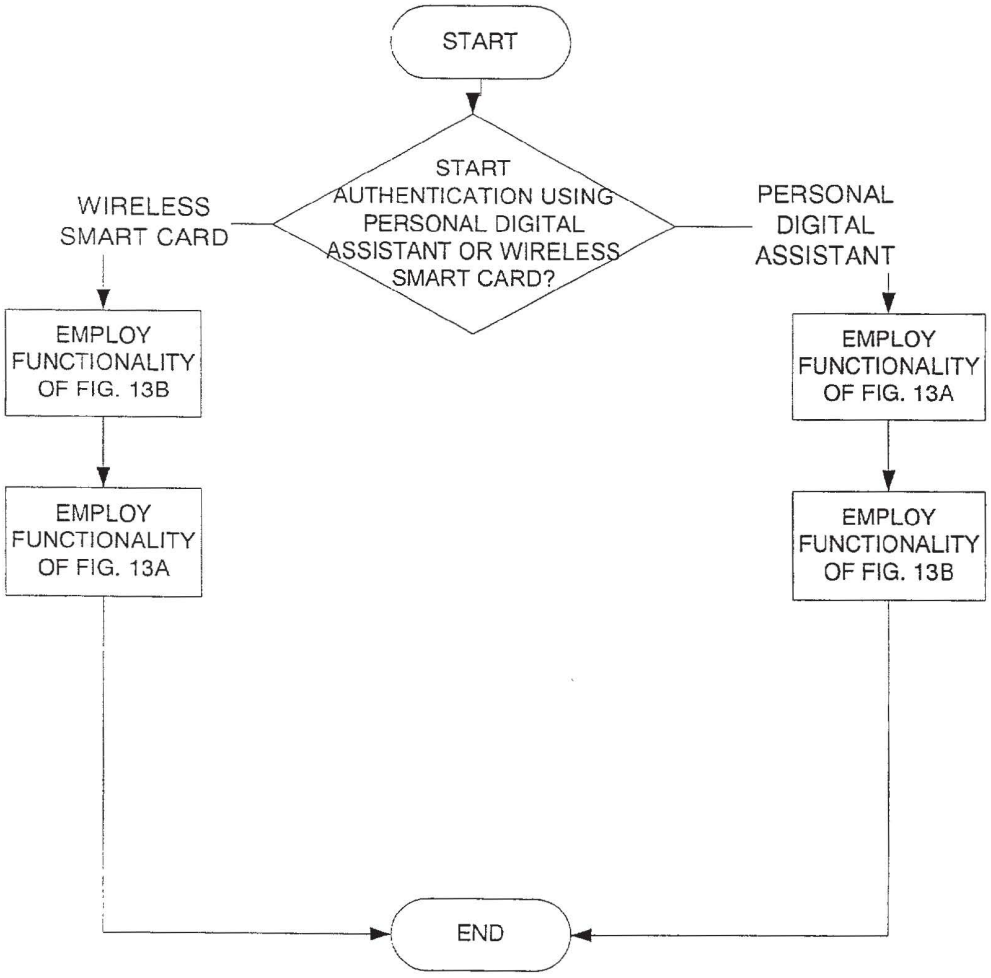

START
START AUTHENTICATION USING PERSONAL DIGITAL ASSISTANT OR WIRELESS SMART CARD?
WIRELESS SMART CARD
PERSONAL DIGITAL ASSISTANT
EMPLOY FUNCTIONALITY OF FIG. 13B
EMPLOY FUNCTIONALITY OF FIG. 13A
EMPLOY FUNCTIONALITY OF FIG. 13A
EMPLOY FUNCTIONALITY OF FIG. 13B
END

FIG. 14F

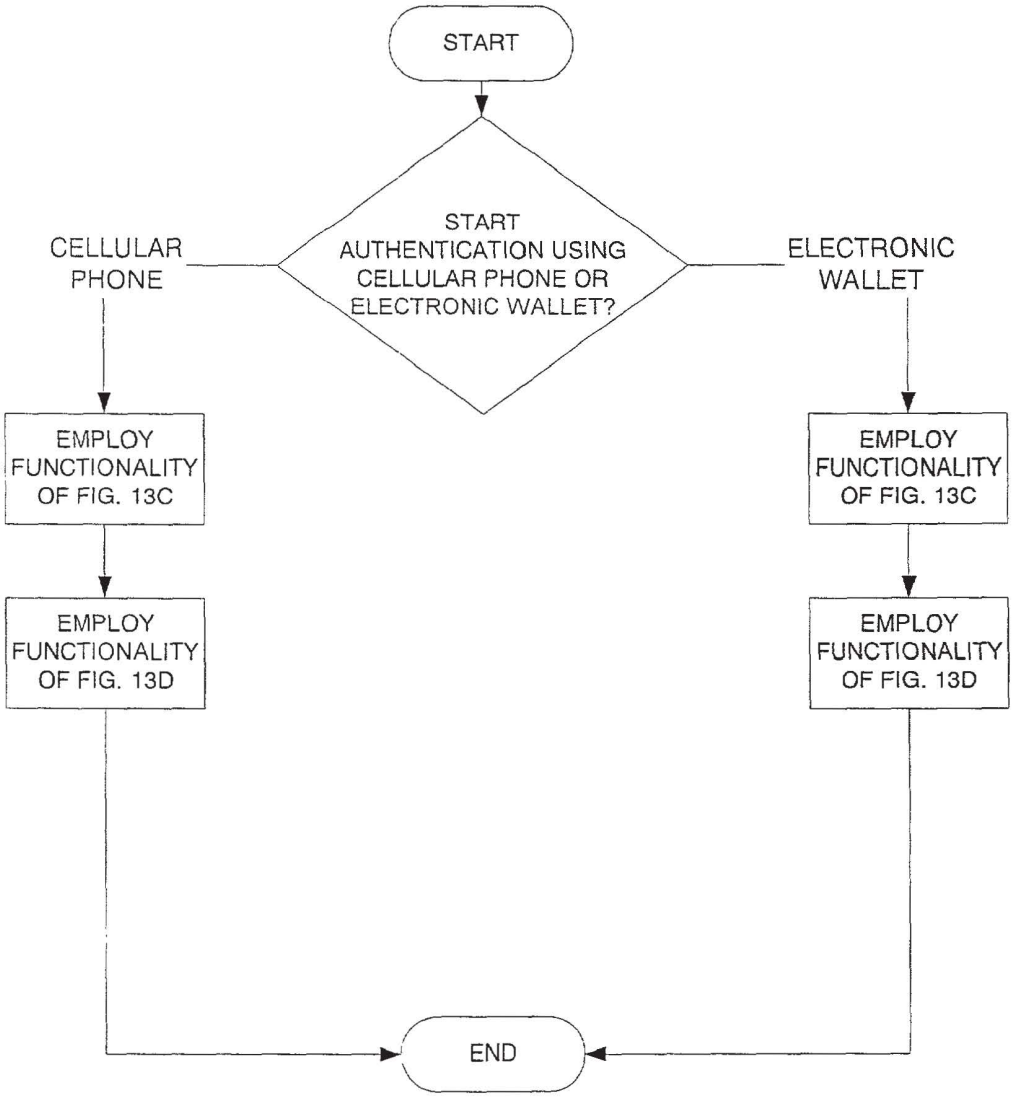

START
START AUTHENTICATION USING CELLULAR PHONE OR ELECTRONIC WALLET?
CELLULAR PHONE
ELECTRONIC WALLET
EMPLOY FUNCTIONALITY OF FIG. 13C
EMPLOY FUNCTIONALITY OF FIG. 13C
EMPLOY FUNCTIONALITY OF FIG. 13D
EMPLOY FUNCTIONALITY OF FIG. 13D
END

FIG. 15A

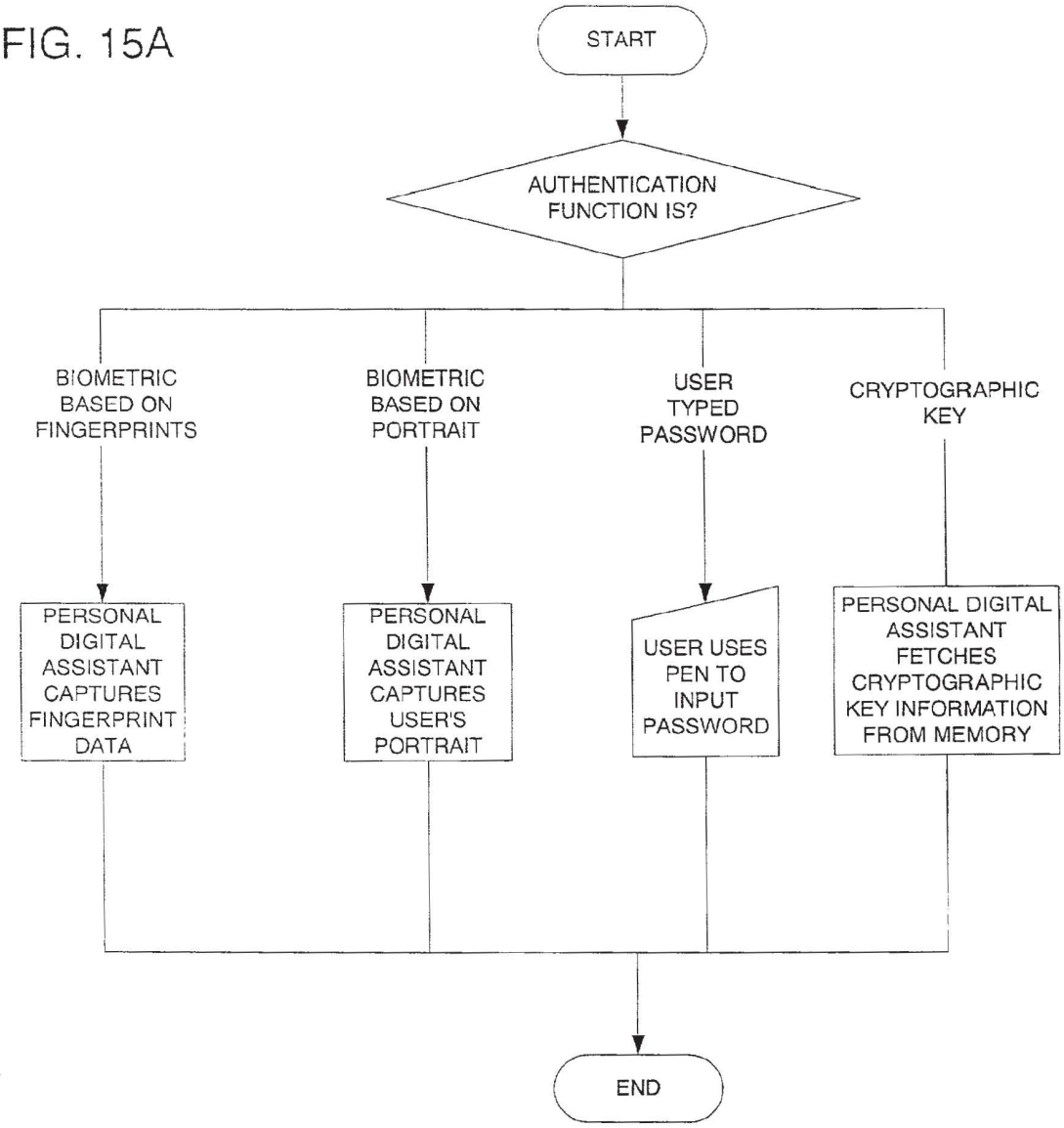

START
AUTHENTICATION FUNCTION IS?
BIOMETRIC BASED ON FINGERPRINTS
BIOMETRIC BASED ON PORTRAIT
USER TYPED PASSWORD
CRYPTOGRAPHIC KEY
PERSONAL DIGITAL ASSISTANT CAPTURES FINGERPRINT DATA
PERSONAL DIGITAL ASSISTANT CAPTURES USER'S PORTRAIT
USER USES PEN TO INPUT PASSWORD
PERSONAL DIGITAL ASSISTANT FETCHES CRYPTOGRAPHIC KEY INFORMATION FROM MEMORY
END

FIG. 15B

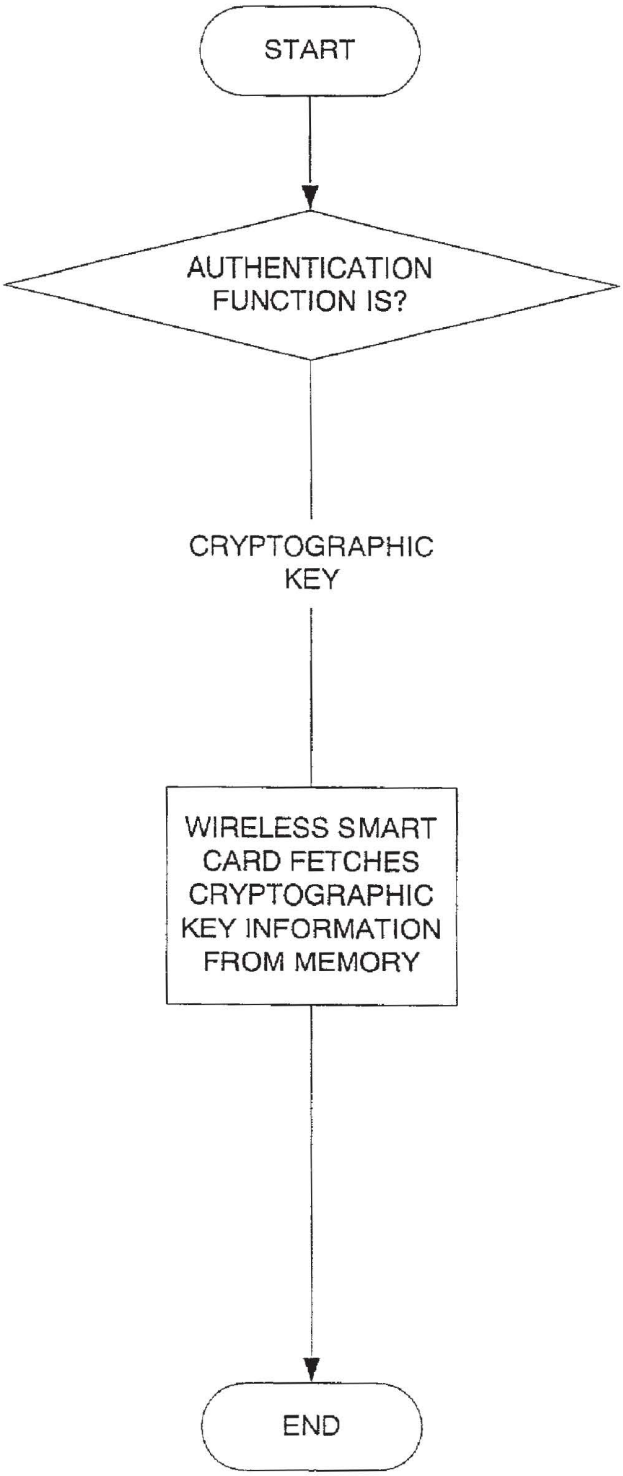

START
AUTHENTICATION FUNCTION IS?
CRYPTOGRAPHIC KEY
WIRELESS SMART CARD FETCHES CRYPTOGRAPHIC KEY INFORMATION FROM MEMORY
END

FIG. 15C

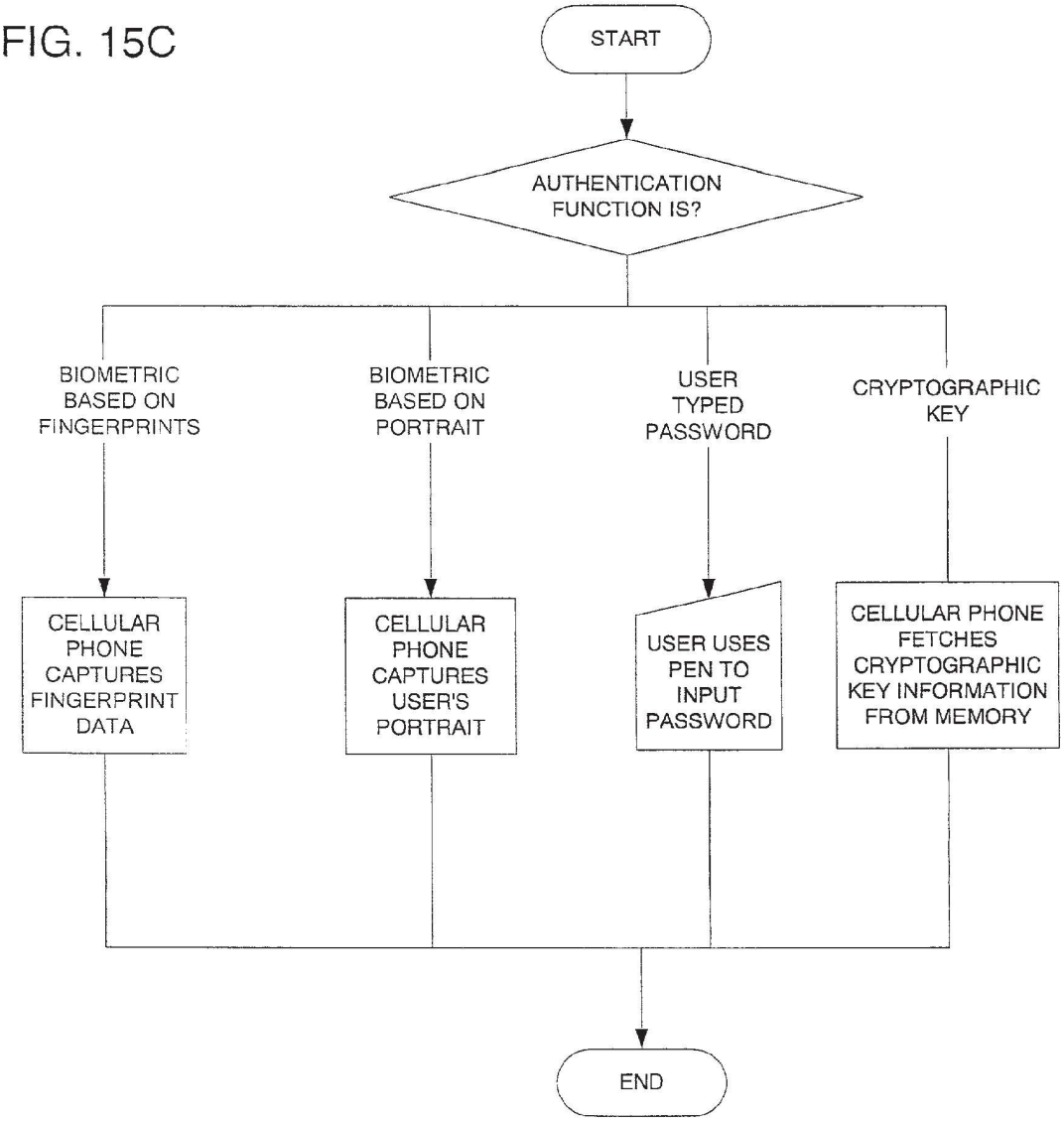

START
AUTHENTICATION FUNCTION IS?
BIOMETRIC BASED ON FINGERPRINTS
BIOMETRIC BASED ON PORTRAIT
USER TYPED PASSWORD
CRYPTOGRAPHIC KEY
CELLULAR PHONE CAPTURES FINGERPRINT DATA
CELLULAR PHONE CAPTURES USER'S PORTRAIT
USER USES PEN TO INPUT PASSWORD
CELLULAR PHONE FETCHES CRYPTOGRAPHIC KEY INFORMATION FROM MEMORY
END

FIG. 15D

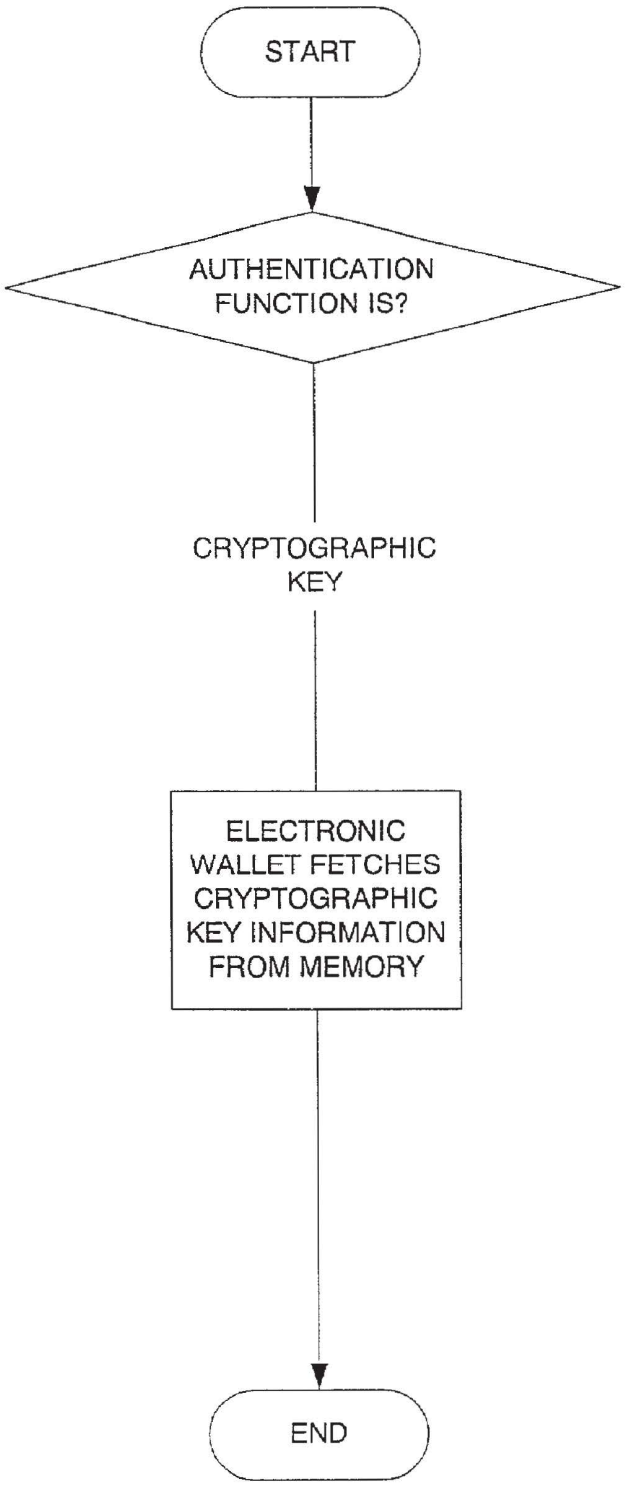

START
AUTHENTICATION FUNCTION IS?
CRYPTOGRAPHIC KEY
ELECTRONIC WALLET FETCHES CRYPTOGRAPHIC KEY INFORMATION FROM MEMORY
END

FIG. 15E

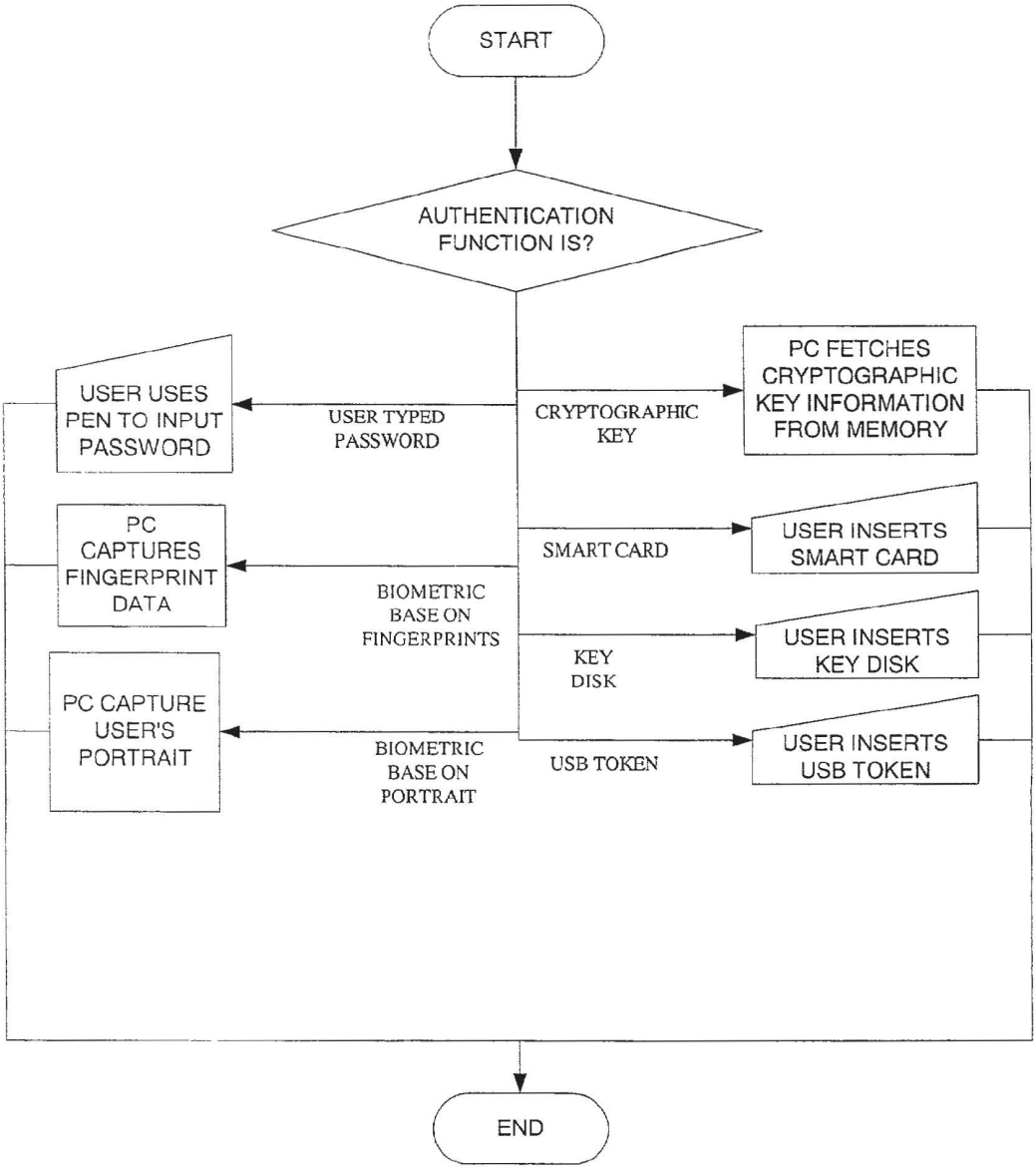

START
AUTHENTICATION FUNCTION IS?
USER USES PEN TO INPUT PASSWORD
USER TYPED PASSWORD
CRYPTOGRAPHIC KEY
PC FETCHES CRYPTOGRAPHIC KEY INFORMATION FROM MEMORY
PC CAPTURES FINGERPRINT DATA
BIOMETRIC BASE ON FINGERPRINTS
SMART CARD
USER INSERTS SMART CARD
KEY DISK
USER INSERTS KEY DISK
PC CAPTURE USER'S PORTRAIT
BIOMETRIC BASE ON PORTRAIT
USB TOKEN
USER INSERTS USB TOKEN
END

FIG. 16A

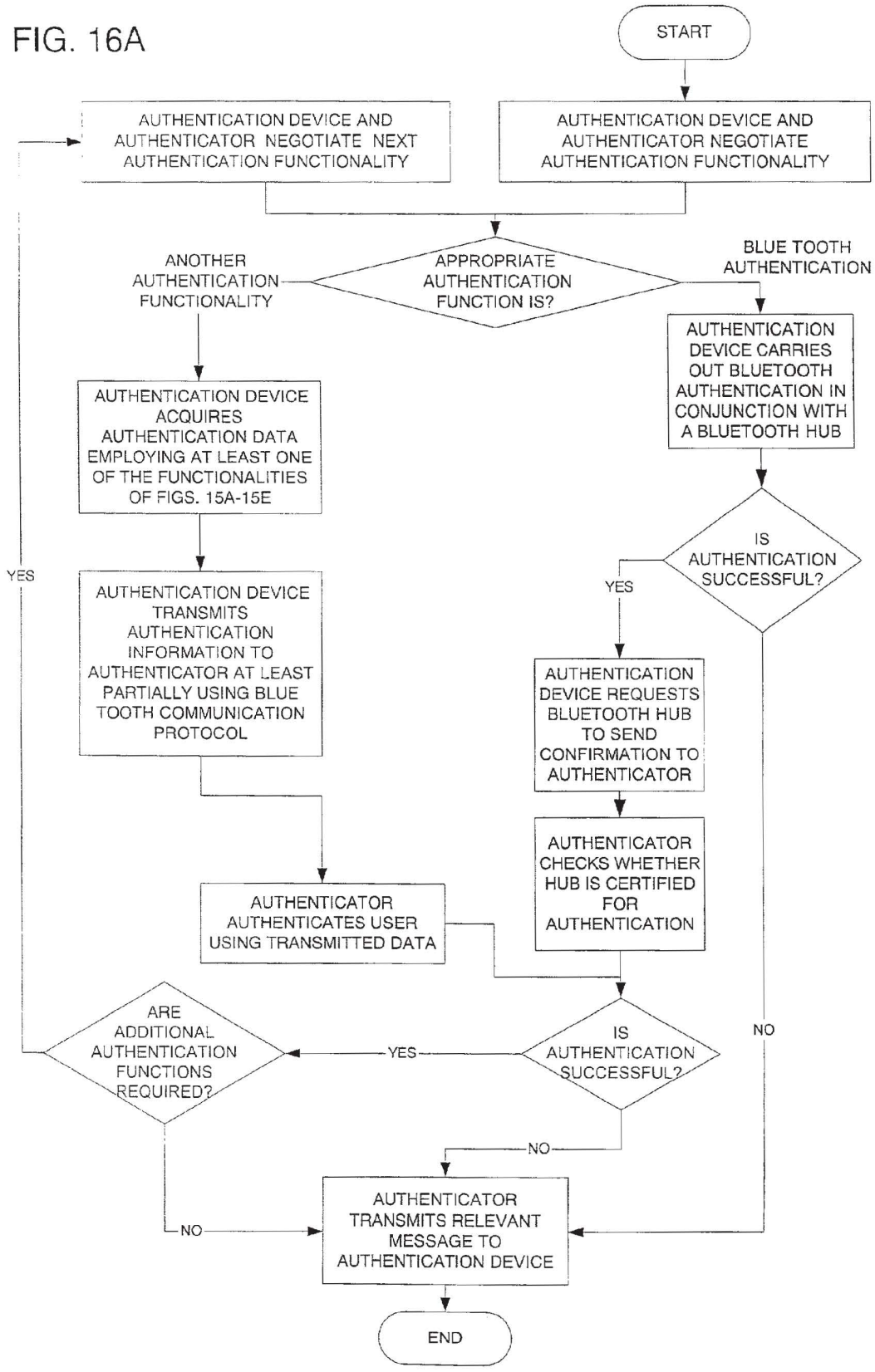

START
AUTHENTICATION DEVICE AND AUTHENTICATOR NEGOTIATE NEXT AUTHENTICATION FUNCTIONALITY
AUTHENTICATION DEVICE AND AUTHENTICATOR NEGOTIATE AUTHENTICATION FUNCTIONALITY
APPROPRIATE AUTHENTICATION FUNCTION IS?
ANOTHER AUTHENTICATION FUNCTIONALITY
BLUE TOOTH AUTHENTICATION
AUTHENTICATION DEVICE ACQUIRES AUTHENTICATION DATA EMPLOYING AT LEAST ONE OF THE FUNCTIONALITIES OF FIGS. 15A-15E
AUTHENTICATION DEVICE CARRIES OUT BLUETOOTH AUTHENTICATION IN CONJUNCTION WITH A BLUETOOTH HUB
IS AUTHENTICATION SUCCESSFUL?
YES
YES
AUTHENTICATION DEVICE TRANSMITS AUTHENTICATION INFORMATION TO AUTHENTICATOR AT LEAST PARTIALLY USING BLUE TOOTH COMMUNICATION PROTOCOL
AUTHENTICATION DEVICE REQUESTS BLUETOOTH HUB TO SEND CONFIRMATION TO AUTHENTICATOR
AUTHENTICATOR CHECKS WHETHER HUB IS CERTIFIED FOR AUTHENTICATION
AUTHENTICATOR AUTHENTICATES USER USING TRANSMITTED DATA
ARE ADDITIONAL AUTHENTICATION FUNCTIONS REQUIRED?
YES
IS AUTHENTICATION SUCCESSFUL?
NO
NO
NO
AUTHENTICATOR TRANSMITS RELEVANT MESSAGE TO AUTHENTICATION DEVICE
END

FIG. 16B

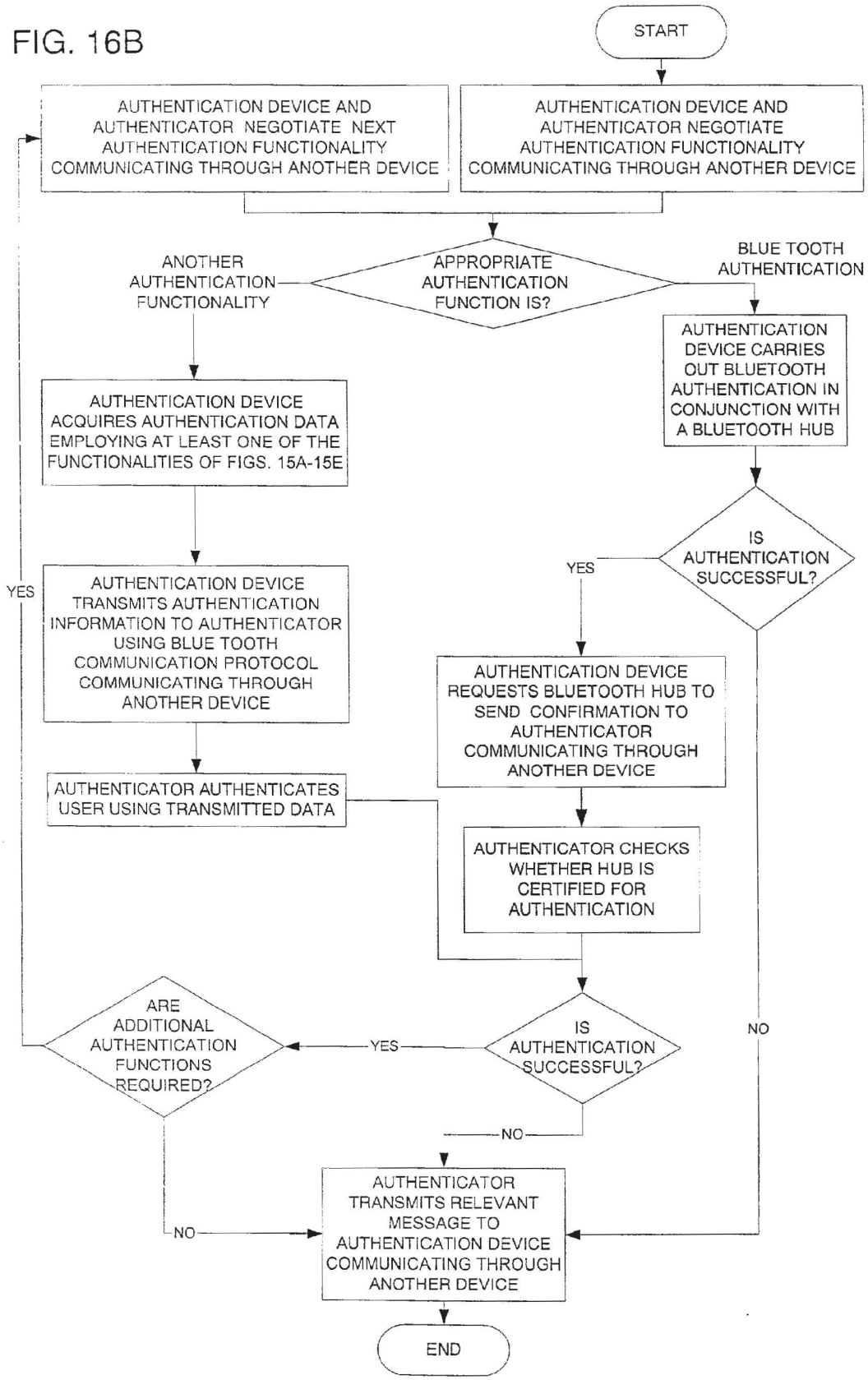

START
AUTHENTICATION DEVICE AND AUTHENTICATOR NEGOTIATE NEXT AUTHENTICATION FUNCTIONALITY COMMUNICATING THROUGH ANOTHER DEVICE
AUTHENTICATION DEVICE AND AUTHENTICATOR NEGOTIATE AUTHENTICATION FUNCTIONALITY COMMUNICATING THROUGH ANOTHER DEVICE
APPROPRIATE AUTHENTICATION FUNCTION IS?
ANOTHER AUTHENTICATION FUNCTIONALITY
BLUE TOOTH AUTHENTICATION
AUTHENTICATION DEVICE ACQUIRES AUTHENTICATION DATA EMPLOYING AT LEAST ONE OF THE FUNCTIONALITIES OF FIGS. 15A-15E
AUTHENTICATION DEVICE CARRIES OUT BLUETOOTH AUTHENTICATION IN CONJUNCTION WITH A BLUETOOTH HUB
IS AUTHENTICATION SUCCESSFUL?
YES
YES
AUTHENTICATION DEVICE TRANSMITS AUTHENTICATION INFORMATION TO AUTHENTICATOR USING BLUE TOOTH COMMUNICATION PROTOCOL COMMUNICATING THROUGH ANOTHER DEVICE
AUTHENTICATION DEVICE REQUESTS BLUETOOTH HUB TO SEND CONFIRMATION TO AUTHENTICATOR COMMUNICATING THROUGH ANOTHER DEVICE
AUTHENTICATOR AUTHENTICATES USER USING TRANSMITTED DATA
AUTHENTICATOR CHECKS WHETHER HUB IS CERTIFIED FOR AUTHENTICATION
ARE ADDITIONAL AUTHENTICATION FUNCTIONS REQUIRED?
YES
IS AUTHENTICATION SUCCESSFUL?
NO
NO
NO
AUTHENTICATOR TRANSMITS RELEVANT MESSAGE TO AUTHENTICATION DEVICE COMMUNICATING THROUGH ANOTHER DEVICE
END

FIG. 16C

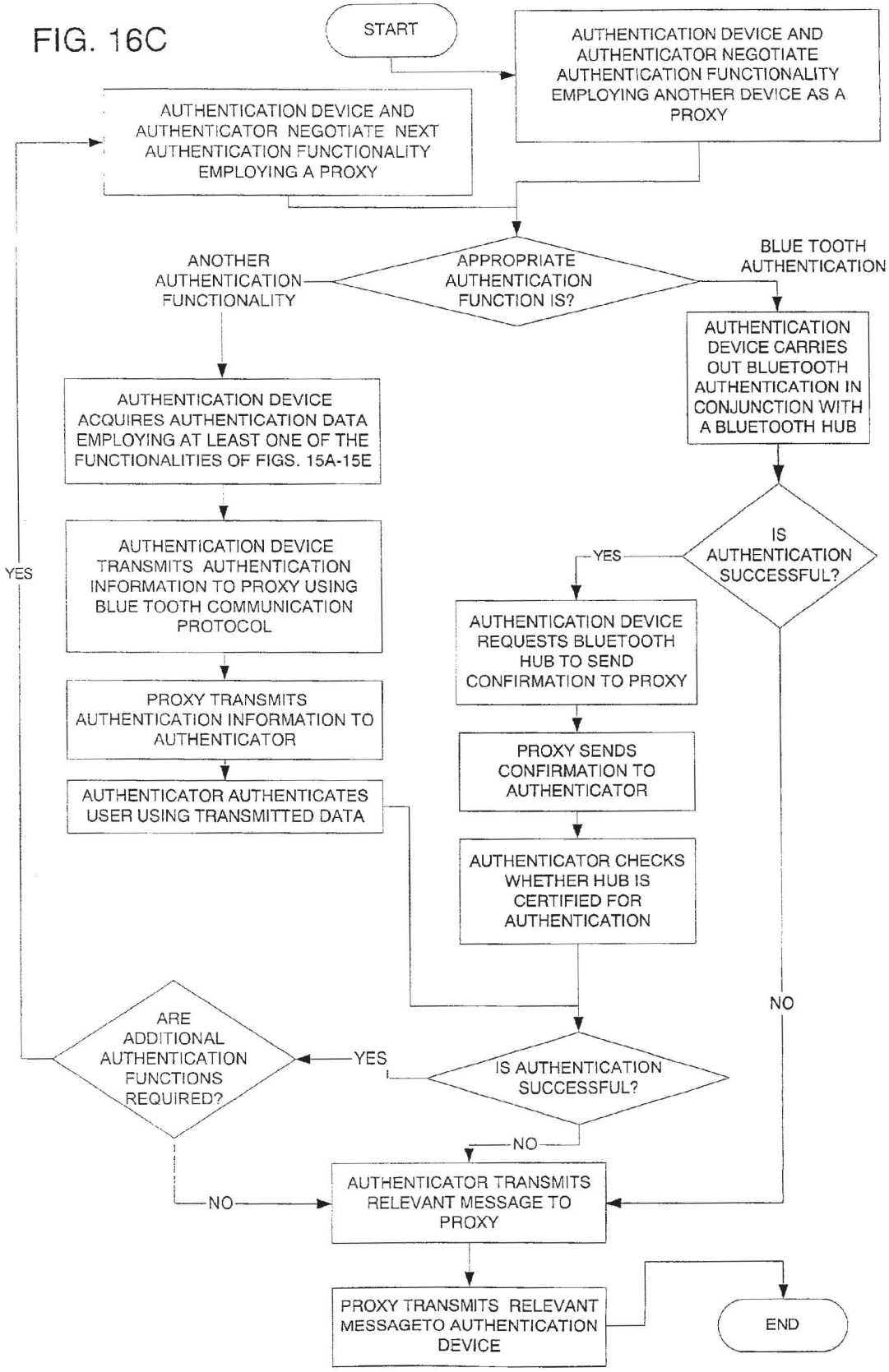

START
AUTHENTICATION DEVICE AND AUTHENTICATOR NEGOTIATE AUTHENTICATION FUNCTIONALITY EMPLOYING ANOTHER DEVICE AS A PROXY
AUTHENTICATION DEVICE AND AUTHENTICATOR NEGOTIATE NEXT AUTHENTICATION FUNCTIONALITY EMPLOYING A PROXY
APPROPRIATE AUTHENTICATION FUNCTION IS?
ANOTHER AUTHENTICATION FUNCTIONALITY
BLUE TOOTH AUTHENTICATION
AUTHENTICATION DEVICE ACQUIRES AUTHENTICATION DATA EMPLOYING AT LEAST ONE OF THE FUNCTIONALITIES OF FIGS. 15A-15E
AUTHENTICATION DEVICE CARRIES OUT BLUETOOTH AUTHENTICATION IN CONJUNCTION WITH A BLUETOOTH HUB
AUTHENTICATION DEVICE TRANSMITS AUTHENTICATION INFORMATION TO PROXY USING BLUE TOOTH COMMUNICATION PROTOCOL
IS AUTHENTICATION SUCCESSFUL?
YES
YES
AUTHENTICATION DEVICE REQUESTS BLUETOOTH HUB TO SEND CONFIRMATION TO PROXY
PROXY TRANSMITS AUTHENTICATION INFORMATION TO AUTHENTICATOR
PROXY SENDS CONFIRMATION TO AUTHENTICATOR
AUTHENTICATOR AUTHENTICATES USER USING TRANSMITTED DATA
AUTHENTICATOR CHECKS WHETHER HUB IS CERTIFIED FOR AUTHENTICATION
NO
ARE ADDITIONAL AUTHENTICATION FUNCTIONS REQUIRED?
YES
IS AUTHENTICATION SUCCESSFUL?
NO
NO
AUTHENTICATOR TRANSMITS RELEVANT MESSAGE TO PROXY
PROXY TRANSMITS RELEVANT MESSAGETO AUTHENTICATION DEVICE
END

FIG. 17A

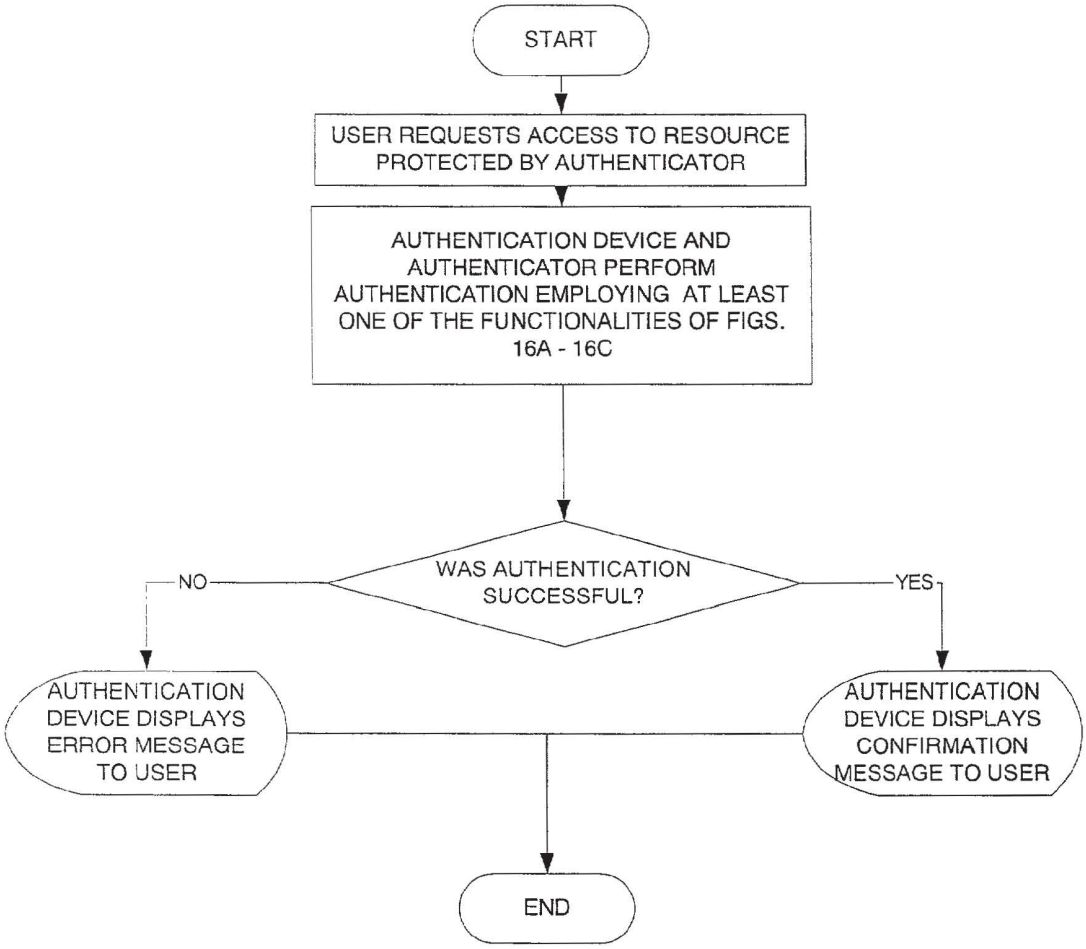

START
USER REQUESTS ACCESS TO RESOURCE PROTECTED BY AUTHENTICATOR
AUTHENTICATION DEVICE AND AUTHENTICATOR PERFORM AUTHENTICATION EMPLOYING AT LEAST ONE OF THE FUNCTIONALITIES OF FIGS. 16A - 16C
WAS AUTHENTICATION SUCCESSFUL?
NO
YES
AUTHENTICATION DEVICE DISPLAYS ERROR MESSAGE TO USER
AUTHENTICATION DEVICE DISPLAYS CONFIRMATION MESSAGE TO USER
END

FIG. 17B

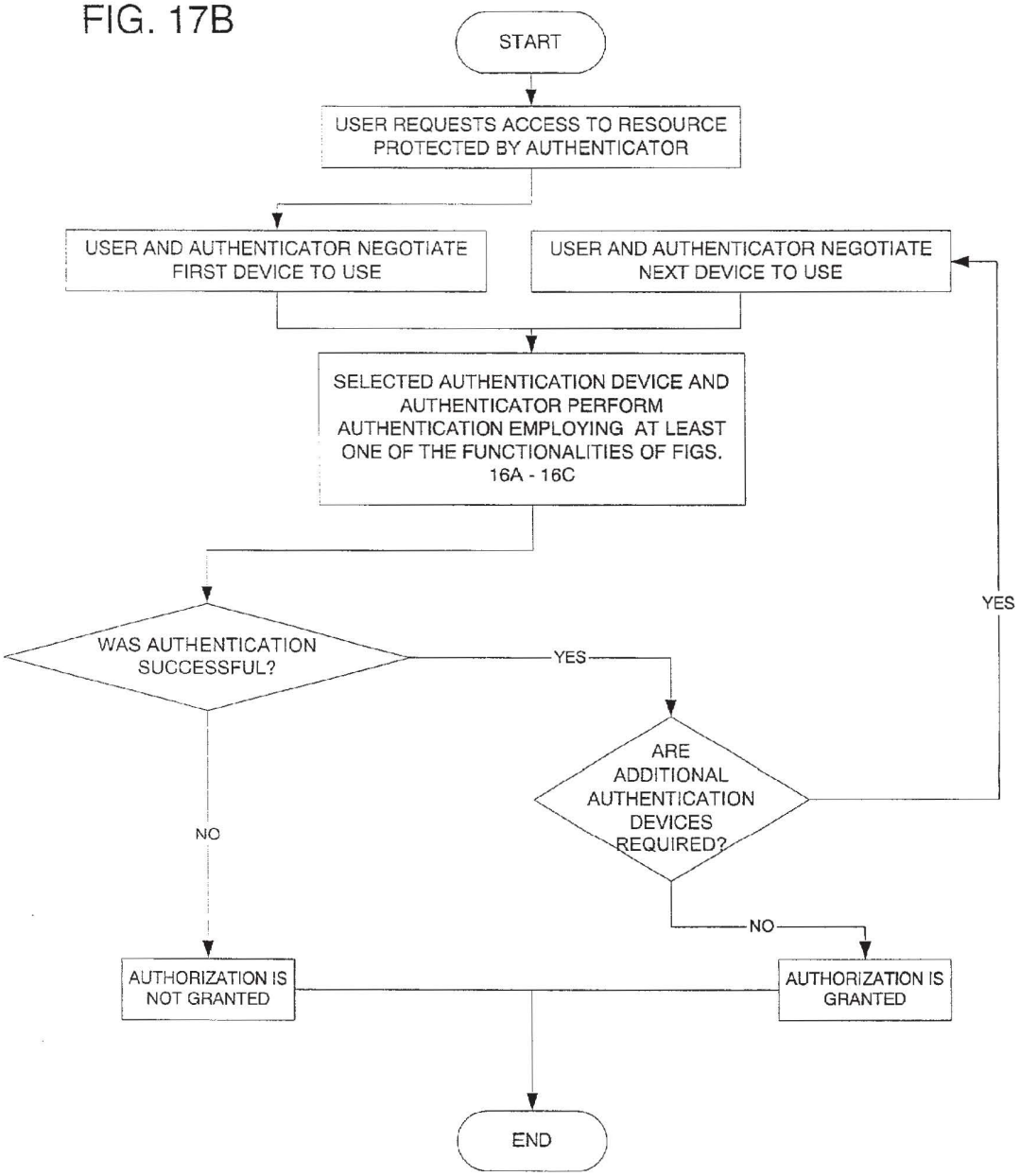
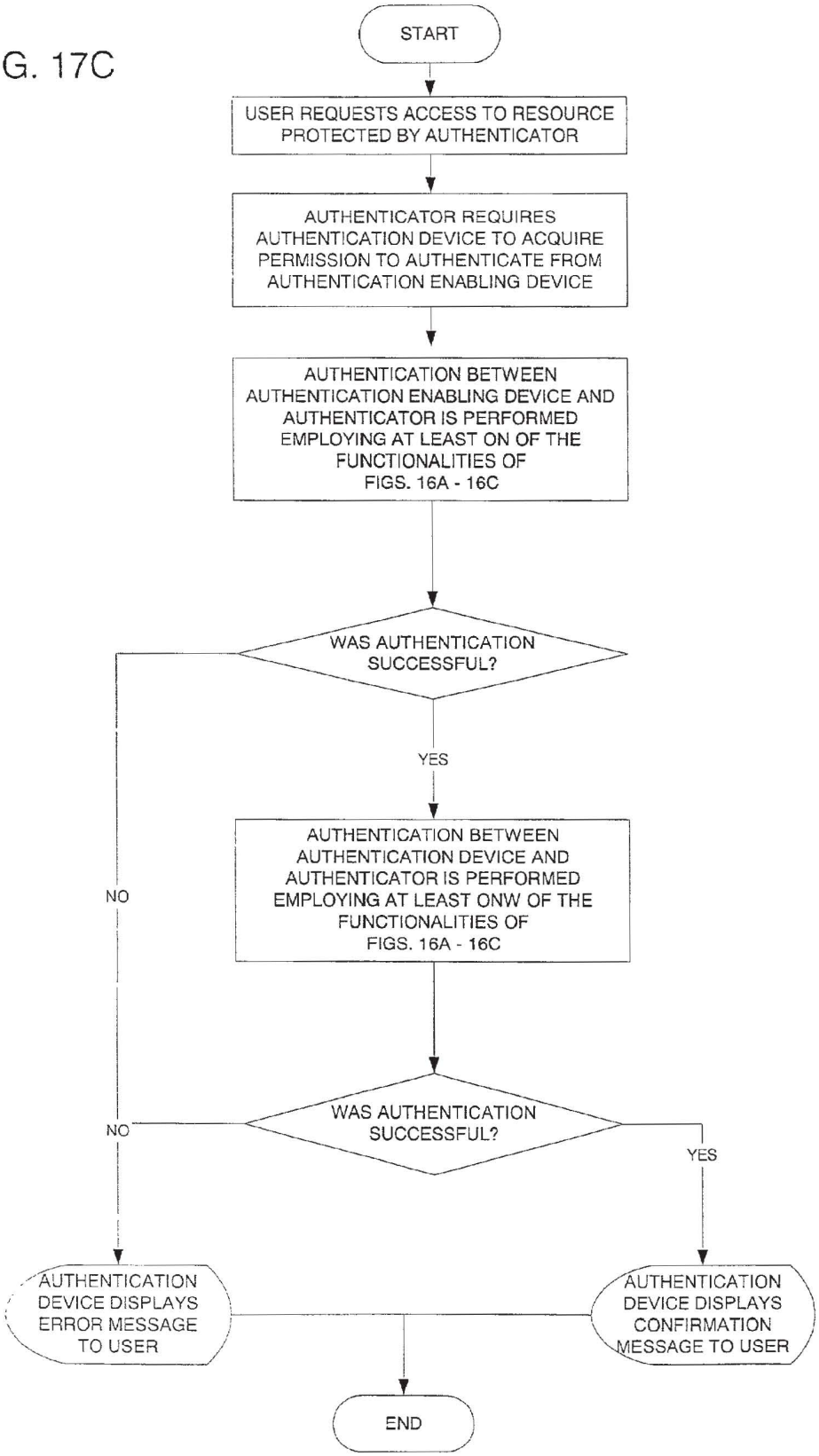

START
USER REQUESTS ACCESS TO RESOURCE PROTECTED BY AUTHENTICATOR
USER AND AUTHENTICATOR NEGOTIATE FIRST DEVICE TO USE
USER AND AUTHENTICATOR NEGOTIATE NEXT DEVICE TO USE
SELECTED AUTHENTICATION DEVICE AND AUTHENTICATOR PERFORM AUTHENTICATION EMPLOYING AT LEAST ONE OF THE FUNCTIONALITIES OF FIGS. 16A - 16C
WAS AUTHENTICATION SUCCESSFUL?
YES
NO
ARE ADDITIONAL AUTHENTICATION DEVICES REQUIRED?
YES
NO
AUTHORIZATION IS NOT GRANTED
AUTHORIZATION IS GRANTED
END

FIG. 17C


START
USER REQUESTS ACCESS TO RESOURCE PROTECTED BY AUTHENTICATOR
AUTHENTICATOR REQUIRES AUTHENTICATION DEVICE TO ACQUIRE PERMISSION TO AUTHENTICATE FROM AUTHENTICATION ENABLING DEVICE
AUTHENTICATION BETWEEN AUTHENTICATION ENABLING DEVICE AND AUTHENTICATOR IS PERFORMED EMPLOYING AT LEAST ON OF THE FUNCTIONALITIES OF FIGS. 16A - 16C
WAS AUTHENTICATION SUCCESSFUL?
YES
NO
AUTHENTICATION BETWEEN AUTHENTICATION DEVICE AND AUTHENTICATOR IS PERFORMED EMPLOYING AT LEAST ONW OF THE FUNCTIONALITIES OF FIGS. 16A - 16C
WAS AUTHENTICATION SUCCESSFUL?
NO
YES
AUTHENTICATION DEVICE DISPLAYS ERROR MESSAGE TO USER
AUTHENTICATION DEVICE DISPLAYS CONFIRMATION MESSAGE TO USER
END

AUTHENTICATION EMPLOYING THE BLUETOOTH COMMUNICATION PROTOCOL

FIELD OF THE INVENTION

[0001] The present invention relates to authentication in computer systems generally.

BACKGROUND OF THE INVENTION

[0002] The following publications are believed to represent the state of the art relevant to the present invention:

[0003] "Bluetooth Security Architecture, Version 1.0" by Thomas Muller, Jul. 15, 1999;

[0004] "Bluetooth specifications core, Version 1.0b", Dec. 1, 1999;

[0005] "Bluetooth specifications profile, Version 1.0b", Dec. 1, 1999;

[0006] "First Access and Bluetooth Announce Technological Collaboration", Feb. 21, 2000;

[0007] "CeBit bluetooth™ pavilion to showcase Ensure's patented XyLoc wireless pc security", Feb. 24, 2000;

[0008] U.S. Pat. No. 6,070,240.

SUMMARY OF THE INVENTION

[0009] There is thus provided in accordance with a preferred embodiment of the present invention a device capable of communicating with an authenticator at least partially using a Bluetooth communication protocol. The device includes at least one authentication functionality, at least part of at least one of which operates to communicate authentication information via the Bluetooth communication protocol.

[0010] There is provided in accordance with another preferred embodiment of the present invention a device capable of communicating with an authenticator. The device includes at least one authentication functionality at least part of at least one of which forms part of the Bluetooth communication protocol.

[0011] There is provided in accordance with a preferred embodiment of the present invention a device capable of communicating with an authenticator at least partially using a Bluetooth communication protocol. The device includes at least one authentication functionality at least part of at least one of which employs a Bluetooth communication protocol.

[0012] There is also provided in accordance with a preferred embodiment of the present invention a system including a communication network, at least one authenticator and at least one device capable of communicating with the authenticator through the communication network, via a Bluetooth communication protocol. The device includes at least one authentication functionality, at least part of at least one of which is operative to communicate authentication information via the Bluetooth communication protocol to the at least one authenticator.

[0013] There is also provided in accordance with yet another preferred embodiment of the present invention a system including a communication network, at least one authenticator and at least one device capable of communicating communicating with the authenticator through the communication network. The device includes at least one authentication functionality, at least part of at least one of which forms part of the Bluetooth communication protocol.

[0014] There is also provided in accordance with a preferred embodiment of the present invention a system including a communication network, at least one authenticator and at least one device capable of communicating with the authenticator through the communication network, via a Bluetooth communication protocol. The device includes at least one authentication functionality at least part of at least one of which employs a Bluetooth communication protocol.

[0015] There is provided in accordance with another preferred embodiment of the present invention a system including at least one authenticator and at least one device capable of communicating with the authenticator via a Bluetooth communication protocol. The device includes at least one authentication functionality, at least part of at least one of which is operative to communicate authentication information via the Bluetooth communication protocol to the authenticator.

[0016] There is further provided in accordance with yet another preferred embodiment of the present invention a system including at least one authenticator and at least one device capable of communicating with the authenticator. The device includes at least one authentication functionality, at least part of at least one of which forms part of the Bluetooth communication protocol.

[0017] There is further provided in accordance with another preferred embodiment of the present invention a system including at least one authenticator and at least one device capable of communicating with the authenticator via a Bluetooth communication protocol. The device includes at least one authentication functionality at least part of at least one of which employs a Bluetooth communication protocol.

[0018] There is provided in accordance with a preferred embodiment of the present invention a system including at least one device and at least one second device. Said system includes at least one multi-tier authentication functionality, at least part of at least one of which operates to communicate authentication information via the Bluetooth communication protocol to at least one authenticator.

[0019] There is provided in accordance with a preferred embodiment of the present invention a system including at least one device and at least one second device. Said system includes at least one multi-tier authentication functionality, at least part of at least one of which forms part of the Bluetooth communication protocol.

[0020] There is provided in accordance with a preferred embodiment of the present invention a system including at least one device and at least one second device. Said system includes at least one multi-tier authentication functionality at least part of at least one of which employs a Bluetooth communication protocol.

[0021] There is further provided in accordance with yet another preferred embodiment of the present invention a method for authenticating with an authenticator. The method includes at least one authentication functionality, at least part of at least one of which is operative to communicate authentication information via the Bluetooth communication protocol.

[0022] There is further provided in accordance with yet another preferred embodiment of the present invention a method for authenticating with an authenticator. The method includes at least one authentication functionality, at least part of at least one of which forms part of the Bluetooth communication protocol.

[0023] There is further provided in accordance with yet another preferred embodiment of the present invention a method for authenticating with an authenticator. The method includes at least one authentication functionality at least part of at least one of which employs a Bluetooth communication protocol.

[0024] Further in accordance with a preferred embodiment of the present invention the device is effective in identifying at least one of the device, another device, a user of the device and the user of the other device, to at least one authenticator coupled to the communication network.

[0025] Additionally in accordance with a preferred embodiment of the present invention the device is a dedicated authentication device.

[0026] Further in accordance with a preferred embodiment of the present invention the device includes substantial non-authentication functionality.

[0027] Preferably, the device includes a telephone, a PDA, a computer, an electronic wallet and a wireless smart card.

[0028] Further in accordance with a preferred embodiment of the present invention the authentication functionality is selected from the following authentication functionalities: a cryptographic authentication functionality, a password based authentication functionality, a smartcard based authentication functionality, a token based authentication functionality and a biometric based authentication functionality.

[0029] Additionaly in accordance with a preferred embodiment of the present invention the authentication functionality forms part of the Bluetooth communication protocol.

[0030] Additionaly in accordance with a preferred embodiment of the present invention the authentication functionality includes at least a plurality of the following authentication functionalities: a cryptographic authentication functionality, a password based authentication functionality, a smartcard based authentication functionality, a token based authentication functionality and a biometric based authentication functionality.

[0031] Additionaly in accordance with a preferred embodiment of the present invention, the authentication functionality includes plural authentication functionalities.

[0032] Preferably, the device includes substantial non-authentication functionality wherein the authentication functionality includes plural authentication functionalities.

[0033] Preferably, the device is a dedicated authentication device and the authentication functionality includes plural authentication functionalities.

BRIEF DESCRIPTION OF THE DRAWINGS

[0034] The present invention will be understood and appreciated more fully from the following detailed description, taken in conjunction with the drawings in which:

[0035] **FIG. 1** is a simplified pictorial illustration of a system and methodology for authentication and communication with a communication network employing a Bluetooth communication protocol in accordance with a preferred embodiment of the present invention;

[0036] **FIG. 2** is a simplified pictorial illustration of a system and methodology for authentication communication with computer employing a Bluetooth communication protocol in accordance with another preferred embodiment of the present invention;

[0037] **FIG. 3** is a simplified pictorial illustration of a system and methodology for multi-tier authentication and communication with a communication network employing a Bluetooth communication protocol in accordance with a preferred embodiment of the present invention;

[0038] **FIG. 4** is a simplified pictorial illustration of a system and methodology for authentication and communication, using a Bluetooth communication protocol, with a communication network in accordance with yet another preferred embodiment of the present invention;

[0039] **FIG. 5** is a simplified pictorial illustration of a system and methodology for authentication and communication, using a Bluetooth communication protocol, with a computer in accordance with yet another preferred embodiment of the present invention;

[0040] **FIG. 6** is a simplified pictorial illustration of a system and methodology for multi-tier authentication and communication, using a Bluetooth communication protocol, with a communication network in accordance with yet another preferred embodiment of the present invention;

[0041] **FIG. 7** is a simplified pictorial illustration of a system and methodology for authentication, using a Bluetooth communication protocol, and communication with a communication network in accordance with yet another preferred embodiment of the present invention;

[0042] **FIG. 8** is a simplified pictorial illustration of a system and methodology for authentication, using a Bluetooth communication protocol, and communication with a computer in accordance with yet another preferred embodiment of the present invention;

[0043] **FIG. 9** is a simplified pictorial illustration of a system and methodology for multi-tier authentication, using a Bluetooth communication protocol, and communication with a communication network in accordance with yet another preferred embodiment of the present invention;

[0044] **FIGS. 10A, 10B**, **10**C, **10**D and **10**E are simplified pictorial illustrations of single authentication functionalities appropriate for five different types of authentication devices;

[0045] **FIGS. 11A, 11B**, **11**C, **11**D, **11**E and **11**F are simplified pictorial illustrations of combinations of authentication functionalities appropriate for six different combinations of different types of authentication devices;

[0046] **FIGS. 12A, 12B** and **12**C are simplified pictorial illustrations of combinations of authentication functionalities appropriate for three different multi-tier combinations of different types of authentication devices;

[0047] **FIGS. 13A, 13B**, **13**C, **13**D and **13**E are simplified flow charts of single authentication functionalities appropri-

ate for five different types of authentication devices and correspond to FIGS. **10**A-**10**E;

[**0048**] **FIGS. 14A, 14B**, **14**C, **14**D, **14**E and **14**F are simplified flow charts of combinations of authentication functionalities appropriate for six different combinations of different types of authentication devices and correspond to FIGS. **11**A-**11**F;

[**0049**] **FIGS. 15A, 15B**, **15**C, **15**D and **15**E are simplified flow charts of methods for obtaining authentication information for five different types of authentication devices;

[**0050**] **FIGS. 16A, 16B** and **16**C are simplified flow charts of various multi-tier and non multi-tier authentication methods using different communication modes between an authenticating device and an authenticator; and

[**0051**] **FIGS. 17A, 17B** and **17**C are simplified flow charts of various multi-tier and non multi-tier authentication methods employing different combinations of authentication devices.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

[**0052**] Reference is now made to **FIG. 1**, which is a simplified pictorial illustration of a system and methodology for communication with a communication network employing a Bluetooth communication protocol in accordance with a preferred embodiment of the present invention. As seen in **FIG. 1**, there is provided an authentication system **100** communicating with a communication network, such as the Internet, herein designated by reference numeral **102** or with an intranet.

[**0053**] For the purposes of the present application "authentication" is to be understood broadly as referring to any process or functionality for providing authorization, access control, permission or approval. The phase "authentication information" is to be understood as any information which is employed for the purpose of authentication.

[**0054**] In accordance with a preferred embodiment of the present invention, the authentication system is effective to identify at least one of at least one device, such as a PC **104**, a telephone **106** and a wireless smart card **108**, and at least one user thereof to at least one authenticator, represented by a lock symbol and designated by reference numeral **110**, coupled to the communication network **102** and arranged to provide an indication of such authentication to other computers, such as those designated by reference numeral **112**, such as web servers, database servers and application servers.

[**0055**] In accordance with one embodiment of the present invention, at least one device, such as PC **104**, communicates with the communication network **102** using a Bluetooth communication protocol, symbolized by a tooth and specifically designated by reference numeral **114**. PC **104** typically includes multiple authentication functionalities, symbolized by multiple keys. As seen in **FIG. 1**, one of the authentication functionalities is a password authentication functionality, designated by reference numeral **116**. Additionally or alternatively a cryptographic authentication functionality may also be provided, such as by means of a USB token **118** which may be associated with the PC **104**.

[**0056**] Additionally in accordance with an embodiment of the present invention, telephone **106** communicates with the communication network **102** in any suitable manner and may or may not employ a Bluetooth communication protocol for communication. In this example, authentication may employ functionality, at least part of which forms part of the Bluetooth communication protocol, as symbolized by a tooth overlaid with a key, collectively designated by reference numeral **120**.

[**0057**] In a further example, a dedicated authentication device, such as the wireless smart card **108** providing access control, communicates with the communication network **102** for authenticating a user thereof and includes cryptographic authentication functionality, symbolized by a key and here specifically designated by reference numeral **122**, which communicates with authenticator **110** using a Bluetooth communication protocol, symbolized by a tooth and specifically designated by reference numeral **124**.

[**0058**] It is appreciated that authentication may be provided in the embodiment of **FIG. 1** by any one or more of the authentication functionalities described hereinabove. Thus authentication may require both Bluetooth authentication functionality and password authentication functionality, provided by telephone **106** and computer **104** respectively.

[**0059**] Reference is now made to **FIG. 2**, which is a simplified pictorial illustration of a system and methodology for authentication employing a Bluetooth communication protocol in accordance with a preferred embodiment of the present invention. As seen in **FIG. 2**, there is provided an authentication system **200** wherein one or more authentication devices communicate with a computer **202**, which itself includes an authenticator **210**.

[**0060**] In accordance with a preferred embodiment of the present invention, the authentication system **200** is effective to identify at least one of at least one authentication device and at least one user thereof to at least one authenticator.

[**0061**] The authentication devices typically include a personal digital assistant **212**, a smart card **214** and an electronic wallet **216**. Personal digital assistant **212** communicates with the computer **202** using a Bluetooth communication protocol, symbolized by a tooth and specifically designated by reference numeral **218** and typically employs a biometric authentication functionality, such as a touch screen fingerprint sensor based authentication functionality, indicated by reference numeral **220**.

[**0062**] Smart card **214** may be a wireless smart card which may employ an authentication functionality at least part of which may form part of the Bluetooth communication protocol, as symbolized by a tooth overlaid with a key, collectively designated by reference numeral **222**.

[**0063**] Electronic wallet **216** communicates with the computer **202** using a Bluetooth communication protocol, symbolized by a tooth and specifically designated by reference numeral **224**. Electronic wallet **216** may employ cryptographic authentication functionality, symbolized by a key and here specifically designated by reference numeral **226**.

[**0064**] It is appreciated that authentication may be provided in the embodiment of **FIG. 2** by any one or more of the authentication devices described hereinabove. Thus a user may be required to provide both biometric inputs and

cryptographic inputs, as by using the personal digital assistant **212** and the electronic wallet **216** respectively.

[**0065**] Reference is now made to **FIG. 3**, which is a simplified pictorial illustration of a system and methodology for multi-tier authentication and communication with a communication network employing a Bluetooth communication protocol in accordance with a preferred embodiment of the present invention.

[**0066**] As seen in **FIG. 3**, there is provided an authentication system **300** communicating with a communication network, such as the Internet, herein designated by reference numeral **302** or with an intranet. System **300** is effective to identify at least one of at least one device, such as a suitably equipped PC **304**, a personal digital assistant **306** and an electronic wallet **308**, and at least one user thereof to at least one authenticator, represented by a lock symbol and designated by reference numeral **310**, coupled to the communication network **302** and arranged to provide an indication of such authentication to other computers, such as those designated by reference numeral **312**, such as web servers, database servers and application servers.

[**0067**] In accordance with a preferred embodiment of the present invention, the authentication system provides multi-tier authentication in that one or more devices, such as personal digital assistant **306**, electronic wallet **308** and PC **304**, which communicate via Bluetooth, are employed in order to authenticate one or more devices or a user thereof to authenticator **310**.

[**0068**] In accordance with one embodiment of the present invention, at least one device, such as PC **304**, communicates with the communication network **302** using a Bluetooth communication protocol, symbolized by a tooth and specifically designated by reference numeral **314**. The at least one device, such as PC **304** may authenticate itself and/or another device or a user to authenticator **310** by means of an authentication functionality at least part of which forms part of the Bluetooth communication protocol.

[**0069**] Additionally or alternatively, the at least one device, such as PC **304** may authenticate itself and/or another device or a user to authenticator **310** by means of a cryptographic authentication functionality, provided such as by means of a key diskette **316**, which may be associated with the at least one device.

[**0070**] The personal digital assistant **306** may communicate with the PC **304** using a Bluetooth communication protocol, symbolized by a tooth and specifically designated by reference numeral **318**. The personal digital assistant **306** may authenticate itself and/or another device or a user to authenticator **310** by means of a password authentication functionality.

[**0071**] The electronic wallet **308** may employ an authentication functionality at least part of which may form part of the Bluetooth communication protocol, as symbolized by a tooth overlaid with a key, collectively designated by reference numeral **320** and may or may not employ a Bluetooth communication protocol for communication.

[**0072**] The multiple-tier authentication functionality of **FIG. 3** may operate in one or more of typically four modes:

[**0073**] The PC **304** may be used merely to communicate to network **302** authentication information sent by personal digital assistant **306**.

[**0074**] The PC **304** may be used as an authentication proxy when suitably enabled by receipt of authentication information from the personal digital assistant **306**.

[**0075**] The PC **304** may be used as an authentication proxy when suitably enabled by receipt of Bluetooth authentication from the electronic wallet **308**.

[**0076**] The personal digital assistant **306** may be used to enable the PC **304** to authenticate itself or a user thereof to the authenticator **310**.

[**0077**] The electronic wallet **308** may be used to enable the PC **304** to authenticate itself or a user thereof to the authenticator **310**.

[**0078**] It is appreciated that authentication may be provided in the embodiment of **FIG. 3** by any one or more of the authentication devices described hereinabove. Thus a user may be required to provide both password inputs and cryptographic inputs, as by using the personal digital assistant **306** and the key diskette **316** respectively.

[**0079**] Reference is now made to **FIG. 4**, which is a simplified pictorial illustration of a system and methodology for communication, using a Bluetooth communication protocol, and authentication with a communication network in accordance with yet another preferred embodiment of the present invention. As seen in **FIG. 4**, there is provided an authentication system **400** communicating with a communication network, such as the Internet, herein designated by reference numeral **402** or with an intranet.

[**0080**] Five different types of devices are shown here in Bluetooth communication via computer network **402** with an authenticator **410**: a wireless smart card **412**, an electronic wallet **414**, a telephone **416**, a personal digital assistant **418** and a PC **420**. It is appreciated that any suitable device may alternatively or additionally communicate via computer network **402** with authenticator **410**.

[**0081**] In accordance with a preferred embodiment of the present invention, the authentication system is effective to identify at least one device or a user thereof to at least one authenticator **410**, represented by a lock symbol, coupled to the communication network **402** and arranged to provide an indication of such authentication to other computers, such as those designated by reference numeral **422**, such as web servers, database servers and application servers.

[**0082**] In accordance with one embodiment of the present invention, at least one device, such as PC **420**, communicates with the communication network **402** using a Bluetooth communication protocol, symbolized by a tooth and specifically designated by reference numeral **424**. PC **420** typically includes multiple authentication functionalities, symbolized by multiple keys associated respectively with a smart card **426**, a key diskette **428** and a USB token **430**. As symbolized by key **432**, the PC **420** may also provide additional authentication functionalities.

[**0083**] Additional devices, such as wireless smart card **412**, electronic wallet **414**, telephone **416** and personal digital assistant **418** each also communicate with the communication network **402** using a Bluetooth communication protocol, as symbolized respectively by a tooth and designated by respective reference numerals **442**, **444**, **446** and **448**. Each such additional device may include a single authentication functionality or multiple authentication functionalities.

[0084] It is appreciated that authentication may be provided in the embodiment of **FIG. 4** by any one or more of the authentication devices and/or functionalities described hereinabove.

[0085] Reference is now made to **FIG. 5**, which is a simplified pictorial illustration of a system and methodology for communication, using a Bluetooth communication protocol, and authentication in accordance with yet another preferred embodiment of the present invention. As seen in **FIG. 5**, there is provided an authentication system **500** wherein one or more authentication devices communicate with a computer **502**, which itself includes an authenticator **510**.

[0086] Four different types of devices are shown here in Bluetooth communication with computer **502** which itself includes authenticator **510**: a wireless smart card **512**, an electronic wallet **514**, a telephone **516** and a personal digital assistant **518**. It is appreciated that any suitable device may alternatively or additionally communicate with computer **502**, which itself includes an authenticator **510**.

[0087] In accordance with a preferred embodiment of the present invention, the authentication system is effective to identify at least one device or a user thereof to at least one authenticator **510**, represented by a lock symbol.

[0088] In accordance with one embodiment of the present invention, at least one device, such as personal digital assistant **518** communicates with the computer **502**, which itself includes an authenticator **510**, using a Bluetooth communication protocol, symbolized by a tooth and specifically designated by reference numeral **524**. Personal digital assistant **518** may include a single authentication functionality or multiple authentication functionalities.

[0089] Additional devices, such as wireless smart card **512**, electronic wallet **514** and telephone **516** each also communicate with the computer **502** using a Bluetooth communication protocol, as symbolized respectively by a tooth and designated by respective reference numerals **542**, **544** and **546**. Each such additional device may include a single authentication functionality or multiple authentication functionalities.

[0090] It is appreciated that authentication may be provided in the embodiment of **FIG. 5** by any one or more of the authentication devices and/or functionalities described hereinabove.

[0091] Reference is now made to **FIG. 6**, which is a simplified pictorial illustration of a system and methodology for communication, using a Bluetooth communication protocol, and authentication with a communication network in accordance with yet another preferred embodiment of the present invention. As seen in **FIG. 6**, there is provided an authentication system **600** communicating with a communication network, such as the Internet, herein designated by reference numeral **602** or with an intranet.

[0092] Four different types of authentication devices are shown here in Bluetooth communication with a computer **604**: a wireless smart card **612**, an electronic wallet **614**, a telephone **616** and a personal digital assistant **618**. It is appreciated that any suitable device may alternatively or additionally communicate with computer **604**, which in turn communicates via network **602** with at least one authenticator **620**, represented by a lock symbol, coupled to the communication network **602** and arranged to provide an indication of such authentication to other computers, such as those designated by reference numeral **622**, such as web servers, database servers and application servers.

[0093] In accordance with a preferred embodiment of the present invention, the authentication system **600** is effective to identify at least one device or a user thereof to at least one authenticator **620**.

[0094] In accordance with a preferred embodiment of the present invention, the authentication system provides multi-tier authentication.

[0095] In accordance with one embodiment of the present invention, at least one authentication device, such as personal digital assistant **618** communicates with the computer **604**, using a Bluetooth communication protocol, symbolized by a tooth and specifically designated by reference numeral **624**. Computer **604** in turn communicates with authenticator **620** via communication network **602**. Personal digital assistant **618** may include a single authentication functionality or multiple authentication functionalities.

[0096] Additional authentication devices, such as wireless smart card **612**, electronic wallet **614** and telephone **616** each also communicate with the computer **604** using a Bluetooth communication protocol, as symbolized respectively by a tooth and designated by respective reference numerals **642**, **644** and **646**. Each such additional device may include a single authentication functionality or multiple authentication functionalities.

[0097] The multiple-tier authentication functionality of **FIG. 6** may operate in one or more of typically three modes:

[0098] The computer **604** may be used merely to communicate to network **602** authentication information sent by any of the above-described authentication devices.

[0099] The computer **604** may be used as an authentication proxy when suitably enabled by receipt of authentication information from the any of the above-described authentication devices.

[0100] Any of the above-described authentication devices may be used to enable the computer **604** to authenticate itself or a user thereof to the authenticator **620**.

[0101] It is appreciated that authentication may be provided in the embodiment of **FIG. 6** by any one or more of the authentication devices and/or functionalities described hereinabove.

[0102] Reference is now made to **FIG. 7**, which is a simplified pictorial illustration of a system and methodology for authentication, using a Bluetooth communication protocol, and communication with a communication network in accordance with yet another preferred embodiment of the present invention. As seen in **FIG. 7**, there is provided an authentication system **700** communicating with a communication network, such as the Internet, herein designated by reference numeral **702** or with an intranet.

[0103] Five different types of devices are shown here in communication via computer network **702** with an authenticator **710**: a wireless smart card **712**, an electronic wallet **714**, a telephone **716**, a personal digital assistant **718** and a PC **720**. It is appreciated that any suitable device may

alternatively or additionally communicate via computer network **702** with authenticator **710**.

[**0104**] In accordance with a preferred embodiment of the present invention, the authentication system is effective to identify at least one device or a user thereof to at least one authenticator **710**, represented by a lock symbol, coupled to the communication network **702** and arranged to provide an indication of such authentication to other computers, such as those designated by reference numeral **722**, such as web servers, database servers and application servers.

[**0105**] In accordance with one embodiment of the present invention, at least one device, such as PC **720**, communicates with the communication network **702**. PC **720** may include one or more authentication functionalities, at least part of at least one of them forming part of a Bluetooth communication protocol, as symbolized by a tooth overlaid by a key and designated by reference numeral **724**.

[**0106**] Additional devices, such as wireless smart card **712**, electronic wallet **714**, telephone **716** and personal digital assistant **718** each also provide authentication via the communication network **702** using an authentication functionality, at least part of which forms part of a Bluetooth communication protocol, as symbolized respectively by a tooth overlaid by a key and designated by respective reference numerals **742**, **744**, **746** and **748**.

[**0107**] It is appreciated that authentication may be provided in the embodiment of **FIG. 7** by any one or more of the authentication devices and/or functionalities described hereinabove.

[**0108**] Reference is now made to **FIG. 8**, which is a simplified pictorial illustration of a system and methodology for authenticating using an authentication functionality, at least part of which forms at least part of a Bluetooth communication protocol in accordance with yet another preferred embodiment of the present invention. As seen in **FIG. 8**, there is provided an authentication system **800** wherein one or more authentication devices communicate with a computer **802**, which itself includes an authenticator **810**.

[**0109**] Four different types of devices are shown here in communication with computer **802** which itself includes authenticator **810**: a wireless smart card **812**, an electronic wallet **814**, a telephone **816** and a personal digital assistant **818**. It is appreciated that any suitable device may alternatively or additionally communicate with computer **802**, which itself includes an authenticator **810**.

[**0110**] In accordance with a preferred embodiment of the present invention, the authentication system is effective to identify at least one device or a user thereof to at least one authenticator **810**, represented by a lock symbol.

[**0111**] In accordance with one embodiment of the present invention, at least one device, such as personal digital assistant **818** communicates with the computer **802**, which itself includes an authenticator **810**, and authenticates to the authenticator **810** employing an authentication functionality, at least part of which forms part of a Bluetooth communication protocol, symbolized by a tooth overlaid by a key and specifically designated by reference numeral **824**.

[**0112**] Additional devices, such as wireless smart card **812**, electronic wallet **814** and telephone **816** each may communicate with the computer **802** and may authenticate using an authentication functionality at least part of which forms part of a Bluetooth communication protocol, as symbolized respectively by a tooth overlaid with a key and designated by respective reference numerals **842**, **844** and **846**.

[**0113**] It is appreciated that authentication may be provided in the embodiment of **FIG. 8** by any one or more of the authentication devices and/or functionalities described hereinabove.

[**0114**] Reference is now made to **FIG. 9**, which is a simplified pictorial illustration of a system and methodology for authentication, using an authentication functionality, at least part of which forms at least part of a Bluetooth communication protocol, via a communication network in accordance with yet another preferred embodiment of the present invention. As seen in **FIG. 9**, there is provided an authentication system **900** communicating with a communication network, such as the Internet, herein designated by reference numeral **902** or with an intranet.

[**0115**] Four different types of authentication devices are shown here in communication with a computer **904**: a wireless smart card **912**, an electronic wallet **914**, a telephone **916** and a personal digital assistant **918**. It is appreciated that any suitable device may alternatively or additionally communicate with computer **904**, which in turn communicates via network **902** with at least one authenticator **920**, represented by a lock symbol, coupled to the communication network **902** and arranged to provide an indication of such authentication to other computers, such as those designated by reference numeral **922**, such as web servers, database servers and application servers.

[**0116**] In accordance with a preferred embodiment of the present invention, the authentication system **900** is effective to identify at least one device or a user thereof to at least one authenticator **920**.

[**0117**] In accordance with a preferred embodiment of the present invention, the authentication system provides multi-tier authentication.

[**0118**] In accordance with one embodiment of the present invention, at least one authentication device, such as personal digital assistant **918**, communicates with the computer **904** and provides authentication using an authentication functionality, at least part of which forms at least part of a Bluetooth communication protocol, symbolized by a tooth overlaid with a key and specifically designated by reference numeral **924**. Computer **904** in turn communicates with authenticator **920** via communication network **902**.

[**0119**] Additional authentication devices, such as wireless smart card **912**, electronic wallet **914** and telephone **916** each may provide authentication using an authentication functionality, at least part of which forms at least part of a Bluetooth communication protocol, as symbolized respectively by a tooth overlaid by a key and designated by respective reference numerals **942**, **944** and **946**.

[**0120**] The multiple-tier authentication functionality of **FIG. 9** may operate in one or more of typically three modes:

[**0121**] The computer **904** may be used merely to communicate to network **902** authentication information sent by any of the above-described authentication devices.

[0122] The computer **904** may be used as an authentication proxy when suitably enabled by receipt of authentication information from the any of the above-described authentication devices.

[0123] Any of the above-described authentication devices may be used to enable the computer **904** to authenticate itself or a user thereof to the authenticator **920**.

[0124] It is appreciated that authentication may be provided in the embodiment of **FIG. 9** by any one or more of the authentication devices and/or functionalities described hereinabove.

[0125] Reference is now made to **FIGS. 10A, 10B**, 10C, **10**D and **10**E which are simplified pictorial illustrations of single authentication functionalities appropriate for five different types of authentication devices and to **FIGS. 13A, 13B, 13**C, **13**D and **13**E, which are simplified flow charts of single authentication functionalities appropriate for five different types of authentication devices and correspond to FIGS. **10**A-**10**E.

[0126] **FIG. 10A** illustrates five different authentication functionalities for a personal digital assistant. As seen in **FIG. 10A, a** personal digital assistant with associated camera, here designated by reference numeral **1000**, provides authentication using facial recognition and communicates with an authenticator **1001**, designated by a lock symbol, typically at least partially using a Bluetooth communication protocol.

[0127] Additionally or alternatively, a personal digital assistant having suitable touch screen functionality and/or an associated camera or scanner here designated by reference numeral **1002**, provides authentication using fingerprint recognition and communicates with authenticator **1001**, typically at least partially using a Bluetooth communication protocol.

[0128] Additionally or alternatively, a personal digital assistant, which may be of conventional design and construction, here designated by reference numeral **1004**, provides password based authentication and communicates with authenticator **1001**, typically at least partially using a Bluetooth communication protocol.

[0129] Additionally or alternatively, a personal digital assistant, which may be of conventional design and construction, here designated by reference numeral **1006**, provides cryptographic authentication and communicates with authenticator **1001**, typically at least partially using a Bluetooth communication protocol.

[0130] Additionally or alternatively, a personal digital assistant, which may be of conventional design and construction, here designated by reference numeral **1008**, provides authentication employing authentication functionality, which forms part of a Bluetooth communication protocol.

[0131] It is appreciated that authentication may be provided in the embodiment of **FIG. 10A** by any one or more of the authentication devices and/or functionalities described hereinabove.

[0132] Reference is now made to **FIG. 13**A, which illustrates the authentication functionalities shown in **FIG. 10A**. As seen in **FIG. 13A, a** user who requests access to a resource protected by an authenticator may employ a personal digital assistant (PDA) to negotiate an authentication functionality. Depending on the facilities available in or in association with the personal digital assistant, one of the following authentication functionalities may be selected:

[0133] biometric utilizing fingerprint recognition;

[0134] biometric utilizing facial recognition;

[0135] password based;

[0136] cryptographic key based; and

[0137] Bluetooth based.

[0138] If the biometric authentication functionality utilizing fingerprint recognition is selected, the personal digital assistant captures the user's fingerprint data.

[0139] If the biometric authentication functionality utilizing facial recognition is selected, the personal digital assistant captures the user's facial features.

[0140] If the password based authentication functionality is selected, the personal digital assistant captures the user password input.

[0141] If the cryptographic key based authentication functionality selected, the personal digital assistant employs a cryptographic key typically stored in its memory.

[0142] In all of the foregoing cases, the personal digital assistant communicates authentication information to the authenticator using the Bluetooth communication protocol. In response to receipt of such information, the authenticator may authenticate the user.

[0143] If the Bluetooth authentication functionality is selected, the personal digital assistant carries out Bluetooth authentication in conjunction with a Bluetooth hub. If the authentication is successful, the personal digital assistant requests that the Bluetooth hub send an authentication confirmation to the authenticator. In response to receipt of the confirmation, the authenticator determines whether the hub, which sent the confirmation, is certified to do so.

[0144] If authentication of the user and/or device is successful, indicating that the user and/or device is authorized, a determination is made as to whether additional authentication functions are required. If so, the personal digital assistant and the authenticator negotiate the next authentication functionality and proceed as described hereinabove. If no additional authentication functions are required, the authenticator transmits an authentication confirmation to the personal digital assistant.

[0145] If authentication of the user and/or device is not successful at any stage, indicating that the user and/or device is not authorized, the authenticator transmits a non-authentication message to the personal digital assistant, which displays a suitable message to the user.

[0146] **FIG. 10B** illustrates two different authentication functionalities for a wireless smart card. As seen in **FIG. 10B, a** wireless smart card, here designated by reference numeral **1010**, provides cryptographic authentication and communicates with an authenticator **1011**, typically at least partially using a Bluetooth communication protocol.

[0147] Additionally or alternatively, a wireless smart card, which may be of conventional design and construction, here designated by reference numeral **1012**, provides authentica-

tion employing authentication functionality, which forms part of a Bluetooth communication protocol.

[0148] It is appreciated that authentication may be provided in the embodiment of **FIG. 10B** by any one or more of the authentication devices and/or functionalities described hereinabove.

[0149] Reference is now made to **FIG. 13**B, which illustrates the authentication functionalities shown in **FIG. 10B**. As seen in **FIG. 13B, a** user who requests access to a resource protected by an authenticator may employ a wireless smart card to negotiate an authentication functionality. Depending on the facilities available in or in association with the wireless smart card, one of the following authentication functionalities may be selected:

[0150] cryptographic key based; and

[0151] Bluetooth based.

[0152] If the cryptographic key based authentication functionality selected, the wireless smart card employs a cryptographic key typically stored in its memory.

[0153] In this case, the wireless smart card communicates authentication information to the authenticator using the Bluetooth communication protocol. In response to receipt of such information, the authenticator may authenticate the user.

[0154] If the Bluetooth authentication functionality is selected, the wireless smart card carries out Bluetooth authentication in conjunction with a Bluetooth hub. If the authentication is successful, the wireless smart card requests that the Bluetooth hub send an authentication confirmation to the authenticator. In response to receipt of the confirmation, the authenticator determines whether the hub, which sent the confirmation, is certified to do so.

[0155] If authentication of the user and/or device is successful, indicating that the user and/or device is authorized, a determination is made as to whether additional authentication functions are required. If so, the wireless smart card and the authenticator negotiate the next authentication functionality and proceed as described hereinabove. If no additional authentication functions are required, the authenticator transmits an authentication confirmation to the wireless smart card.

[0156] If authentication of the user and/or device is not successful at any stage, indicating that the user and/or device is not authorized, the authenticator transmits a non-authentication message to the wireless smart card, which communicates a suitable message to the user.

[0157] **FIG. 10C** illustrates five different authentication functionalities for a cellular phone. As seen in **FIG. 10C, a** cellular phone with associated camera, here designated by reference numeral **1020**, provides authentication using facial recognition and communicates with an authenticator **1021**, designated by a lock symbol, typically at least partially using a Bluetooth communication protocol.

[0158] Additionally or alternatively, a cellular phone having suitable touch screen functionality and/or an associated camera or scanner here designated by reference numeral **1022**, provides authentication using fingerprint recognition and/or facial recognition and communicates with authenticator **1021**, typically at least partially using a Bluetooth communication protocol.

[0159] Additionally or alternatively, a cellular phone, which may be of conventional design and construction, here designated by reference numeral **1024**, provides password based authentication and communicates with authenticator **1021**, typically at least partially using a Bluetooth communication protocol.

[0160] Additionally or alternatively, a cellular phone, which may be of conventional design and construction, here designated by reference numeral **1026**, provides cryptographic authentication and communicates with authenticator **1021**, typically at least partially using a Bluetooth communication protocol.

[0161] Additionally or alternatively, a cellular phone, which may be of conventional design and construction, here designated by reference numeral **1028**, provides authentication employing authentication functionality, which forms part of a Bluetooth communication protocol.

[0162] It is appreciated that authentication may be provided in the embodiment of **FIG. 10C** by any one or more of the authentication devices and/or functionalities described hereinabove.

[0163] Reference is now made to **FIG. 13**C, which illustrates the authentication functionalities shown in **FIG. 10C**. As seen in **FIG. 13C, a** user who requests access to a resource protected by an authenticator may employ a cellular phone to negotiate an authentication functionality. Depending on the facilities available in or in association with the cellular phone, one of the following authentication functionalities may be selected:

[0164] biometric utilizing fingerprint recognition;

[0165] biometric utilizing facial recognition;

[0166] password based;

[0167] cryptographic key based; and

[0168] Bluetooth based.

[0169] If the biometric authentication functionality utilizing fingerprint recognition is selected, the cellular phone captures the user's fingerprint data.

[0170] If the biometric authentication functionality utilizing facial recognition is selected, the cellular phone captures the user's facial features.

[0171] If the password based authentication functionality is selected, the cellular phone captures the user password input.

[0172] If the cryptographic key based authentication functionality selected, the cellular phone employs a cryptographic key typically stored in its memory.

[0173] In all of the foregoing cases, the cellular phone communicates authentication information to the authenticator using the Bluetooth communication protocol. In response to receipt of such information, the authenticator may authenticate the user.

[0174] If the Bluetooth authentication functionality is selected, the cellular phone carries out Bluetooth authenti-

cation in conjunction with a Bluetooth hub. If the authentication is successful, the cellular phone requests that the Bluetooth hub send an authentication confirmation to the authenticator. In response to receipt of the confirmation, the authenticator determines whether the hub, which sent the confirmation, is certified to do so.

[0175] If authentication of the user and/or device is successful, indicating that the user and/or device is authorized, a determination is made as to whether additional authentication functions are required. If so, the cellular phone and the authenticator negotiate the next authentication functionality and proceed as described hereinabove. If no additional authentication functions are required, the authenticator transmits an authentication confirmation to the cellular phone.

[0176] If authentication of the user and/or device is not successful at any stage, indicating that the user and/or device is not authorized, the authenticator transmits a non-authentication message to the cellular phone, which displays a suitable message to the user.

[0177] **FIG. 10D** illustrates two different authentication functionalities for an electronic wallet. As seen in **FIG. 10**D, an electronic wallet, here designated by reference numeral **1030**, provides cryptographic authentication and communicates with an authenticator **1031**, typically at least partially using a Bluetooth communication protocol.

[0178] Additionally or alternatively, an electronic wallet, which may be of conventional design and construction, here designated by reference numeral **1032**, provides authentication employing authentication functionality, which forms part of a Bluetooth communication protocol.

[0179] It is appreciated that authentication may be provided in the embodiment of **FIG. 10D** by any one or more of the authentication devices and/or functionalities described hereinabove.

[0180] Reference is now made to **FIG. 13**D, which illustrates the authentication functionalities shown in **FIG. 10D**. As seen in **FIG. 13D, a** user who requests access to a resource protected by an authenticator may employ an electronic wallet to negotiate an authentication functionality. Depending on the facilities available in or in association with the electronic wallet, one of the following authentication functionalities may be selected:

[0181] cryptographic key based; and

[0182] Bluetooth based.

[0183] If the cryptographic key based authentication functionality selected, the electronic wallet employs a cryptographic key typically stored in its memory.

[0184] In this case, the electronic wallet communicates authentication information to the authenticator using the Bluetooth communication protocol. In response to receipt of such information, the authenticator may authenticate the user.

[0185] If the Bluetooth authentication functionality is selected, the electronic wallet carries out Bluetooth authentication in conjunction with a Bluetooth hub. If the authentication is successful, the electronic wallet requests that the Bluetooth hub send an authentication confirmation to the authenticator. In response to receipt of the confirmation, the authenticator determines whether the hub, which sent the confirmation, is certified to do so.

[0186] If authentication of the user and/or device is successful, indicating that the user and/or device is authorized, a determination is made as to whether additional authentication functions are required. If so, the electronic wallet and the authenticator negotiate the next authentication functionality and proceed as described hereinabove. If no additional authentication functions are required, the authenticator transmits an authentication confirmation to the electronic wallet.

[0187] If authentication of the user and/or device is not successful at any stage, indicating that the user and/or device is not authorized, the authenticator transmits a non-authentication message to the electronic wallet, which communicates a suitable message to the user.

[0188] **FIG. 10E** illustrates eight different authentication functionalities for a PC. As seen in **FIG. 10E, a** PC with associated camera, here designated by reference numeral **1040**, provides authentication using facial recognition and communicates with an authenticator **1041**, designated by a lock symbol, typically at least partially using a Bluetooth communication protocol.

[0189] Additionally or alternatively, a PC having suitable touch screen functionality and/or an associated camera or scanner here designated by reference numeral **1042**, provides authentication using fingerprint recognition and communicates with authenticator **1041**, typically at least partially using a Bluetooth communication protocol.

[0190] Additionally or alternatively, a PC, which may be of conventional design and construction, here designated by reference numeral **1043**, provides password based authentication and communicates with authenticator **1041**, typically at least partially using a Bluetooth communication protocol.

[0191] Additionally or alternatively, a PC which may be of conventional design and construction, here designated by reference numeral **1044**, provides cryptographic authentication and communicates with authenticator **104-1**, typically employing a memory based key, typically at least partially using a Bluetooth communication protocol.

[0192] Additionally or alternatively, a PC with an associated suitable USB token, here designated by reference numeral **1045**, provides cryptographic authentication and communicates with authenticator **1041**, typically at least partially using a Bluetooth communication protocol.

[0193] Additionally or alternatively, a PC with associated smart card, here designated by reference numeral **1047**, provides cryptographic authentication and communicates with authenticator **1041**, typically at least partially using a Bluetooth communication protocol.

[0194] Additionally or alternatively, a PC with an associated suitable key diskette, here designated by reference numeral **1046**, provides cryptographic authentication and communicates with authenticator **1041**, typically at least partially using a Bluetooth communication protocol.

[0195] Additionally or alternatively, a PC, which may be of conventional design and construction, here designated by

reference numeral **1048**, provides authentication employing authentication functionality, which forms part of a Bluetooth communication protocol.

[**0196**] It is appreciated that authentication may be provided in the embodiment of **FIG. 10E** by any one or more of the authentication devices and/or functionalities described hereinabove.

[**0197**] Reference is now made to **FIG. 13**E, which illustrates the authentication functionalities shown in **FIG. 10E**. As seen in **FIG. 13E, a** user who requests access to a resource protected by an authenticator may employ a PC to negotiate an authentication functionality. Depending on the facilities available in or in association with the PC, one of the following authentication functionalities may be selected:

[**0198**] biometric utilizing fingerprint recognition;

[**0199**] biometric utilizing facial recognition;

[**0200**] password based;

[**0201**] cryptographic utilizing a memory based key;

[**0202**] cryptographic utilizing a USB token based key;

[**0203**] cryptographic utilizing a smart card based key;

[**0204**] cryptographic utilizing a diskette based key; and

[**0205**] Bluetooth based.

[**0206**] If the biometric authentication functionality utilizing fingerprint recognition is selected, the PC captures the user's fingerprint data.

[**0207**] If the biometric authentication functionality utilizing facial recognition is selected, the PC captures the user's facial features.

[**0208**] If the password based authentication functionality is selected, the PC captures the user password input.

[**0209**] If the cryptographic memory based key authentication functionality is selected, the PC employs a cryptographic key typically stored in its memory.

[**0210**] If the cryptographic USB token based key authentication functionality is selected, the PC employs a cryptographic key typically stored in the associated USB key.

[**0211**] If the cryptographic smart card based key authentication functionality is selected, the PC employs a cryptographic key typically stored in the associated smart card.

[**0212**] If the cryptographic diskette based key authentication functionality is selected, the PC employs a cryptographic key typically stored in the associated key diskette.

[**0213**] In all of the foregoing cases, the PC communicates authentication information to the authenticator using the Bluetooth communication protocol. In response to receipt of such information, the authenticator may authenticate the user.

[**0214**] If the Bluetooth authentication functionality is selected, the PC carries out Bluetooth authentication in conjunction with a Bluetooth hub. If the authentication is successful, the PC requests that the Bluetooth hub send an authentication confirmation to the authenticator. In response to receipt of the confirmation, the authenticator determines whether the hub, which sent the confirmation, is certified to do so.

[**0215**] If authentication of the user and/or device is successful, indicating that the user and/or device is authorized, a determination is made as to whether additional authentication functions are required. If so, the PC and the authenticator negotiate the next authentication functionality and proceed as described hereinabove. If no additional authentication functions are required, the authenticator transmits an authentication confirmation to the PC.

[**0216**] If authentication of the user and/or device is not successful at any stage, indicating that the user and/or device is not authorized, the authenticator transmits a non-authentication message to the PC, which displays a suitable message to the user.

[**0217**] Reference is now made to **FIGS. 11A, 11B**, 11C, 11D, 11E and 11F which are simplified pictorial illustrations of combinations of authentication functionalities appropriate for six different combinations of different types of authentication devices and to **FIGS. 14A, 14B**, 14C, 14D, 14E and 14F, which are simplified flow charts of combinations of authentication functionalities appropriate for six different types of authentication devices and correspond to FIGS. 11A-11F.

[**0218**] **FIG. 11A** illustrates two different authentication functionalities for a wireless smart card, here designated by reference numeral **1100** and three different authentication functionalities for a PC with associated camera or scanner, here designated by reference numeral **1102**. The five different functionalities may be combined in any combination of two or more functionalities to provide authentication in conjunction with an authenticator **1103**, designated by a lock symbol, typically at least partially using a Bluetooth communication protocol.

[**0219**] As seen in **FIG. 11**A, wireless smart card **1100** provides cryptographic authentication functionality and communicates with authenticator **1103**, typically at least partially using a Bluetooth communication protocol.

[**0220**] Additionally or alternatively, wireless smart card **1100** provides authentication employing authentication functionality, which forms part of a Bluetooth communication protocol.

[**0221**] Additionally or alternatively, the PC having an associated camera or scanner **1102**, provides biometric authentication functionality using typically one or both of facial recognition and fingerprint recognition and communicates with authenticator **1103**, typically at least partially using a Bluetooth communication protocol.

[**0222**] Additionally or alternatively, the PC **1102** provides password based authentication functionality and communicates with authenticator **1103**, typically at least partially using a Bluetooth communication protocol.

[**0223**] It is appreciated that authentication may be provided in the embodiment of **FIG. 11A** by any one or more of the authentication devices and/or functionalities described hereinabove.

[**0224**] Reference is now made to **FIG. 14**A, which illustrates the authentication functionalities shown in **FIG. 11A**.

As seen in **FIG. 14A, a** user employs the functionalities of **FIGS. 13B and 13E** typically in series in order to provide authentication. The user preferably negotiates with an authenticator to determine whether the functionality of **FIG. 13B** is employed prior to that of **FIG. 13E** or vice versa.

[0225] **FIG. 11B** illustrates three different authentication functionalities for a cellular phone with associated camera, here designated by reference numeral **1110** and four different authentication functionalities for a PC with associated camera or scanner, here designated by reference numeral **1112**. The seven different functionalities may be combined in any combination of two or more functionalities to provide authentication in conjunction with an authenticator **1113**, designated by a lock symbol, typically at least partially using a Bluetooth communication protocol.

[0226] As seen in **FIG. 11**B, cellular phone with associated camera **1110** provides biometric authentication functionality utilizing facial recognition and communicates with authenticator **1113**, typically at least partially using a Bluetooth communication protocol.

[0227] Additionally or alternatively cellular phone **1110**, which may be of conventional design and construction, provides password based authentication functionality and communicates with authenticator **1113**, typically at least partially using a Bluetooth communication protocol.

[0228] Additionally or alternatively cellular phone **1110**, which may be of conventional design and construction, provides authentication employing authentication functionality, which forms part of a Bluetooth communication protocol.

[0229] Additionally or alternatively, the PC having an associated camera or scanner **1112** provides biometric authentication functionality utilizing fingerprint recognition and communicates with authenticator **1113**, typically at least partially using a Bluetooth communication protocol.

[0230] Additionally or alternatively, the PC **1112** provides password based authentication functionality and communicates with authenticator **1113**, typically at least partially using a Bluetooth communication protocol.

[0231] Additionally or alternatively, the PC **1112** provides cryptographic authentication functionality utilizing a diskette based key and communicates with authenticator **1113**, typically at least partially using a Bluetooth communication protocol.

[0232] Additionally or alternatively, the PC **1112** provides cryptographic authentication functionality utilizing USB token based key and communicates with authenticator **1113**, typically at least partially using a Bluetooth communication protocol.

[0233] It is appreciated that authentication may be provided in the embodiment of **FIG. 11B** by any one or more of the authentication devices and/or functionalities described hereinabove.

[0234] Reference is now made to **FIG. 14**B, which illustrates the authentication functionalities shown in **FIG. 11B**. As seen in **FIG. 14B, a** user employs the functionalities of **FIGS. 13C and 13E** typically in series in order to provide authentication. The user preferably negotiates with an authenticator to determine whether the functionality of **FIG. 13C** is employed prior to that of **FIG. 13E** or vice versa.

[0235] **FIG. 11C** illustrates four different authentication functionalities for a personal digital assistant having suitable touch screen functionality and/or an associated camera or scanner, here designated by reference numeral **1120** and four different authentication functionalities for a PC with associated camera or scanner, here designated by reference numeral **1122**. The eight different functionalities may be combined in any combination of two or more functionalities to provide authentication in conjunction with an authenticator **1123**, designated by a lock symbol, typically at least partially using a Bluetooth communication protocol. **[0110]**

[0236] As seen in **FIG. 11**C, personal digital assistant having suitable touch screen functionality and/or an associated camera or scanner **1120** provides biometric authentication functionality utilizing fingerprint recognition and communicates with authenticator **1123**, typically at least partially using a Bluetooth communication protocol.

[0237] Additionally or alternatively personal digital assistant **1120**, which may be of conventional design and construction, provides password based authentication functionality and communicates with authenticator **1123**, typically at least partially using a Bluetooth communication protocol.

[0238] Additionally or alternatively personal digital assistant **1120**, which may be of conventional design and construction, provides cryptographic authentication functionality and communicates with authenticator **1123**, typically at least partially using a Bluetooth communication protocol.

[0239] Additionally or alternatively personal digital assistant **1120**, which may be of conventional design and construction, provides authentication employing authentication functionality, which forms part of a Bluetooth communication protocol.

[0240] Additionally or alternatively, a PC having an associated camera or scanner **1122**, provides biometric authentication functionality using typically fingerprint recognition and communicates with authenticator **1123**, typically at least partially using a Bluetooth communication protocol.

[0241] Additionally or alternatively, the PC **1122**, which may be of conventional design and manufacturing, provides password based authentication functionality and communicates with authenticator **1123**, typically at least partially using a Bluetooth communication protocol.

[0242] Additionally or alternatively, the PC **1122** with associated smart card provides cryptographic authentication functionality utilizing smart card based key and communicates with authenticator **1123**, typically at least partially using a Bluetooth communication protocol.

[0243] Additionally or alternatively, the PC **1122**, which may be of conventional design and manufacturing, provides cryptographic authentication functionality utilizing memory based key authentication and communicates with authenticator **1123**, typically at least partially using a Bluetooth communication protocol.

[0244] It is appreciated that authentication may be provided in the embodiment of **FIG. 11C** by any one or more of the authentication devices and/or functionalities described hereinabove.

[0245] Reference is now made to **FIG. 14**C, which illustrates the authentication functionalities shown in **FIG. 11C**. As seen in **FIG. 14C, a** user employs the functionalities of **FIGS. 13A and 13E** typically in series in order to provide authentication. The user preferably negotiates with an authenticator to determine whether the functionality of **FIG. 13A** is employed prior to that of **FIG. 13E** or vice versa.

[0246] **FIG. 11D** illustrates four different authentication functionalities for a personal digital assistant having suitable touch screen functionality and/or an associated camera or scanner, here designated by reference numeral **1130** and three different authentication functionalities for a cellular phone with associated camera or scanner, here designated by reference numeral **1132**. The seven different functionalities may be combined in any combination of two or more functionalities to provide authentication in conjunction with an authenticator **1133**, designated by a lock symbol, typically at least partially using a Bluetooth communication protocol.

[0247] As seen in **FIG. 11**D, personal digital assistant having suitable touch screen functionality and/or an associated camera or scanner **1130** provides biometric authentication functionality utilizing fingerprint recognition and communicates with authenticator **1133**, typically at least partially using a Bluetooth communication protocol.

[0248] Additionally or alternatively personal digital assistant **1130**, which may be of conventional design and construction, provides password based authentication functionality and communicates with authenticator **1133**, typically at least partially using a Bluetooth communication protocol.

[0249] Additionally or alternatively personal digital assistant **1130**, which may be of conventional design and construction, provides cryptographic authentication functionality and communicates with authenticator **1133**, typically at least partially using a Bluetooth communication protocol.

[0250] Additionally or alternatively personal digital assistant **1130**, which may be of conventional design and construction, provides authentication employing authentication functionality, which forms part of a Bluetooth communication protocol.

[0251] Additionally or alternatively, a cellular phone having an associated camera or scanner **1132** provides biometric authentication functionality using typically facial recognition and communicates with authenticator **1133**, typically at least partially using a Bluetooth communication protocol.

[0252] Additionally or alternatively, the cellular phone **1132**, which may be of conventional design and manufacturing, provides password based authentication functionality and communicates with authenticator **1133**, typically at least partially using a Bluetooth communication protocol.

[0253] Additionally or alternatively cellular phone **1132**, which may be of conventional design and construction, provides authentication employing authentication functionality, which forms part of a Bluetooth communication protocol.

[0254] It is appreciated that authentication may be provided in the embodiment of **FIG. 11D** by any one or more of the authentication devices and/or functionalities described hereinabove.

[0255] Reference is now made to **FIG. 14**D, which illustrates the authentication functionalities shown in **FIG. 11D**. As seen in **FIG. 14D, a** user employs the functionalities of **FIGS. 13A and 13C** typically in series in order to provide authentication. The user preferably negotiates with an authenticator to determine whether the functionality of **FIG. 13A** is employed prior to that of **FIG. 13C** or vice versa.

[0256] **FIG. 11E** illustrates three different authentication functionalities for a personal digital assistant having suitable touch screen functionality and/or an associated camera or scanner, here designated by reference numeral **1140** and two different authentication functionalities for a wireless smart card, here designated by reference numeral **1142**. The five different functionalities may be combined in any combination of two or more functionalities to provide authentication in conjunction with an authenticator **1143**, designated by a lock symbol, typically at least partially using a Bluetooth communication protocol.

[0257] As seen in **FIG. 11**E, personal digital assistant having suitable touch screen functionality and/or an associated camera or scanner **1140** provides biometric authentication functionality utilizing fingerprint recognition and communicates with authenticator **1143**, typically at least partially using a Bluetooth communication protocol.

[0258] Additionally or alternatively personal digital assistant **1140**, which may be of conventional design and construction, provides password based authentication functionality and communicates with authenticator **1143**, typically at least partially using a Bluetooth communication protocol.

[0259] Additionally or alternatively personal digital assistant **1140**, which may be of conventional design and construction, provides authentication employing authentication functionality, which forms part of a Bluetooth communication protocol.

[0260] Additionally or alternatively wireless smart card **1142** provides cryptographic authentication functionality and communicates with authenticator **1143**, typically at least partially using a Bluetooth communication protocol.

[0261] Additionally or alternatively wireless smart card **1142**, which may be of conventional design and construction, provides authentication employing authentication functionality, which forms part of a Bluetooth communication protocol.

[0262] It is appreciated that authentication may be provided in the embodiment of **FIG. 11E** by any one or more of the authentication devices and/or functionalities described hereinabove.

[0263] Reference is now made to **FIG. 14**E, which illustrates the authentication functionalities shown in **FIG. 11E**. As seen in **FIG. 14E, a** user employs the functionalities of **FIGS. 13A and 13B** typically in series in order to provide authentication. The user preferably negotiates with an authenticator to determine whether the functionality of **FIG. 13A** is employed prior to that of **FIG. 13B** or vice versa.

[0264] **FIG. 11F** illustrates two different authentication functionalities for an electronic wallet, here designated by reference numeral **1150** and four different authentication functionalities for a cellular phone having an associated camera or scanner, here designated by reference numeral **1152**. The five different functionalities may be combined in