any combination of two or more functionalities to provide authentication in conjunction with an authenticator **1153**, designated by a lock symbol, typically at least partially using a Bluetooth communication protocol.

[**0265**] As seen in **FIG. 11**F, wireless smart card **1152** provides cryptographic authentication functionality and communicates with authenticator **1153**, typically at least partially using a Bluetooth communication protocol.

[**0266**] Additionally or alternatively wireless smart card **1152**, which may be of conventional design and construction, provides authentication employing authentication functionality, which forms part of a Bluetooth communication protocol.

[**0267**] Additionally or alternatively cellular phone having an associated camera or scanner **1152** provides biometric authentication functionality employing typically facial and/or fingerprint recognition and communicates with authenticator **1153**, typically at least partially using a Bluetooth communication protocol.

[**0268**] Additionally or alternatively cellular phone **1152**, which may be of conventional design and manufacturing, provides password based authentication functionality and communicates with authenticator **1153**, typically at least partially using a Bluetooth communication protocol.

[**0269**] Additionally or alternatively cellular phone **1152**, which may be of conventional design and construction, provides authentication employing authentication functionality, which forms part of a Bluetooth communication protocol.

[**0270**] It is appreciated that authentication may be provided in the embodiment of **FIG. 11F** by any one or more of the authentication devices and/or functionalities described hereinabove.

[**0271**] Reference is now made to **FIG. 14**F, which illustrates the authentication functionalities shown in **FIG. 11F**. As seen in **FIG. 14F, a** user employs the functionalities of **FIGS. 13C and 13D** 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. 13D** or vice versa.

[**0272**] Reference is now made to **FIGS. 12A, 12B** and **12**C, which are simplified pictorial illustrations of combinations of authentication functionalities appropriate for three different types of multi-tier authentication systems.

[**0273**] **FIG. 12A** illustrates four different authentication functionalities for a PC with associated camera or scanner, here designated by reference numeral **1200**, four different authentication functionalities for a personal digital assistant with suitable touch screen functionality and/or an associated camera or scanner, here designated by reference numeral **1202** and two different authentication functionalities for a wireless smart card, here designated by reference numeral **1204**. The ten different functionalities may be combined in any combination of two or more functionalities to provide multi-tier authentication in conjunction with an authenticator **1205**, designated by a lock symbol, typically at least partially using a Bluetooth communication protocol.

[**0274**] As seen in **FIG. 12A** a PC having an associated camera or scanner **1200**, provides biometric authentication functionality using typically fingerprint recognition and communicates with authenticator **1205**, typically at least partially using a Bluetooth communication protocol.

[**0275**] Additionally or alternatively, the PC **1200**, which may be of conventional design and manufacturing, provides password based authentication functionality and communicates with authenticator **1205**, typically at least partially using a Bluetooth communication protocol.

[**0276**] Additionally or alternatively, the PC **1200** with associated USB token provides cryptographic authentication functionality utilizing USB token based key and communicates with authenticator **1205**, typically at least partially using a Bluetooth communication protocol.

[**0277**] Additionally or alternatively, the PC **1200**, which may be of conventional design and manufacturing, provides cryptographic authentication functionality utilizing memory based key authentication and communicates with authenticator **1205**, typically at least partially using a Bluetooth communication protocol.

[**0278**] Additionally or alternatively, personal digital assistant having suitable touch screen functionality and/or an associated camera or scanner **1202** provides biometric authentication functionality utilizing fingerprint recognition and communicates with authenticator **1205**, typically at least partially using a Bluetooth communication protocol.

[**0279**] Additionally or alternatively personal digital assistant **1202**, which may be of conventional design and construction, provides password based authentication functionality and communicates with authenticator **1205**, typically at least partially using a Bluetooth communication protocol.

[**0280**] Additionally or alternatively personal digital assistant **1202**, which may be of conventional design and construction, provides cryptographic authentication functionality and communicates with authenticator **1205**, typically at least partially using a Bluetooth communication protocol.

[**0281**] Additionally or alternatively personal digital assistant **1202**, which may be of conventional design and construction, provides authentication employing authentication functionality, which forms part of a Bluetooth communication protocol.

[**0282**] Additionally or alternatively wireless smart card **1204** provides cryptographic authentication functionality and communicates with authenticator **1205**, typically at least partially using a Bluetooth communication protocol.

[**0283**] Additionally or alternatively, wireless smart card **1204** provides authentication employing authentication functionality, which forms part of a Bluetooth communication protocol.

[**0284**] It is appreciated that multi-tier authentication may be provided in the embodiment of **FIG. 12A** by any one or more combinations of the authentication devices and/or functionalities described hereinabove.

[**0285**] **FIG. 12B** illustrates four different authentication functionalities for a personal digital assistant with suitable touch screen functionality and/or associated camera or scanner, here designated by reference numeral **1210**, four different authentication functionalities for a cellular phone with an associated camera or scanner, here designated by reference numeral **1212** and two different authentication func-

tionalities for an electronic wallet, here designated by reference numeral **1214**. The ten different functionalities may be combined in any combination of two or more functionalities to provide multi-tier authentication in conjunction with an authenticator **1215**, designated by a lock symbol, typically at least partially using a Bluetooth communication protocol.

[**0286**] As seen in **FIG. 12B** personal digital assistant having suitable touch screen functionality and/or an associated camera or scanner **1210** provides biometric authentication functionality utilizing fingerprint recognition and communicates with authenticator **1215**, typically at least partially using a Bluetooth communication protocol.

[**0287**] Additionally or alternatively personal digital assistant **1210**, which may be of conventional design and construction, provides password based authentication functionality and communicates with authenticator **1215**, typically at least partially using a Bluetooth communication protocol.

[**0288**] Additionally or alternatively personal digital assistant **1210**, which may be of conventional design and construction, provides cryptographic authentication functionality and communicates with authenticator **1215**, typically at least partially using a Bluetooth communication protocol.

[**0289**] Additionally or alternatively personal digital assistant **1210**, which may be of conventional design and construction, provides authentication employing authentication functionality, which forms part of a Bluetooth communication protocol.

[**0290**] Additionally or alternatively cellular phone with associated camera, here designated by reference numeral **1212**, provides authentication using facial recognition and communicates with an authenticator **1215**, designated by a lock symbol, typically at least partially using a Bluetooth communication protocol.

[**0291**] Additionally or alternatively, a cellular phone, which may be of conventional design and construction, here designated by reference numeral **1212**, provides password based authentication and communicates with authenticator **1215**, typically at least partially using a Bluetooth communication protocol.

[**0292**] Additionally or alternatively, cellular phone, which may be of conventional design and construction, here designated by reference numeral **1212**, provides cryptographic authentication and communicates with authenticator **1215**, typically at least partially using a Bluetooth communication protocol.

[**0293**] Additionally or alternatively, cellular phone, which may be of conventional design and construction, here designated by reference numeral **1212**, provides authentication employing authentication functionality, which forms part of a Bluetooth communication protocol.

[**0294**] Additionally or alternatively, electronic wallet, here designated by reference numeral **1214**, provides cryptographic authentication and communicates with an authenticator **1215**, typically at least partially using a Bluetooth communication protocol.

[**0295**] Additionally or alternatively, electronic wallet, which may be of conventional design and construction, here designated by reference numeral **1214**, provides authentication employing authentication functionality, which forms part of a Bluetooth communication protocol.

[**0296**] It is appreciated that multi-tier authentication may be provided in the embodiment of **FIG. 12B** by any one or more combinations of the authentication devices and/or functionalities described hereinabove.

[**0297**] **FIG. 12C** illustrates four different authentication functionalities for a cellular phone with suitable touch screen functionality and/or associated camera or scanner, here designated by reference numeral **1220**, four different authentication functionalities for a personal digital assistant with a suitable touch screen and/or an associated camera or scanner, here designated by reference numeral **1222**, four different authentication functionalities for a PC with a suitable touch screen and an associated camera or scanner, here designated by reference numeral **1224**, and two different authentication functionalities for a wireless smart card, here designated by reference numeral **1226**. The fourteen different functionalities may be combined in any combination of two or more functionalities to provide multi-tier authentication in conjunction with an authenticator **1227**, designated by a lock symbol, typically at least partially using a Bluetooth communication protocol.

[**0298**] As seen in **FIG. 12C** cellular phone with associated camera, here designated by reference numeral **1220**, provides authentication using facial recognition and communicates with an authenticator **1227**, designated by a lock symbol, typically at least partially using a Bluetooth communication protocol.

[**0299**] Additionally or alternatively, a cellular phone, which may be of conventional design and construction, here designated by reference numeral **1220**, provides password based authentication and communicates with authenticator **1227**, typically at least partially using a Bluetooth communication protocol.

[**0300**] Additionally or alternatively, cellular phone, which may be of conventional design and construction, here designated by reference numeral **1220**, provides cryptographic authentication and communicates with authenticator **1227**, typically at least partially using a Bluetooth communication protocol.

[**0301**] Additionally or alternatively, cellular phone, which may be of conventional design and construction, here designated by reference numeral **1220**, provides authentication employing authentication functionality, which forms part of a Bluetooth communication protocol.

[**0302**] Additionally or alternatively, personal digital assistant having suitable touch screen functionality and/or an associated camera or scanner **1222** provides biometric authentication functionality utilizing fingerprint recognition and communicates with authenticator **1227**, typically at least partially using a Bluetooth communication protocol.

[**0303**] Additionally or alternatively personal digital assistant **1222**, which may be of conventional design and construction, provides password based authentication functionality and communicates with authenticator **1227**, typically at least partially using a Bluetooth communication protocol.

[**0304**] Additionally or alternatively personal digital assistant **1222**, which may be of conventional design and construction, provides cryptographic authentication functional-

ity and communicates with authenticator **1227**, typically at least partially using a Bluetooth communication protocol.

[**0305**] Additionally or alternatively personal digital assistant **1222**, which may be of conventional design and construction, provides authentication employing authentication functionality, which forms part of a Bluetooth communication protocol.

[**0306**] Additionally or alternatively the PC having an associated camera or scanner **1224**, provides biometric authentication functionality using typically fingerprint recognition and communicates with authenticator **1227**, typically at least partially using a Bluetooth communication protocol.

[**0307**] Additionally or alternatively, PC **1224**, which may be of conventional design and manufacturing, provides password based authentication functionality and communicates with authenticator **1227**, typically at least partially using a Bluetooth communication protocol.

[**0308**] Additionally or alternatively, PC **1224**, which may be of conventional design and manufacturing, provides cryptographic authentication functionality utilizing suitable key diskette authentication and communicates with authenticator **1227**, typically at least partially using a Bluetooth communication protocol.

[**0309**] Additionally or alternatively, PC **1224**, which may be of conventional design and manufacturing, provides authentication employing authentication functionality, which forms part of a Bluetooth communication protocol.

[**0310**] Additionally or alternatively wireless smart card **1226** provides cryptographic authentication functionality and communicates with authenticator **1227**, typically at least partially using a Bluetooth communication protocol.

[**0311**] Additionally or alternatively, wireless smart card **1226** provides authentication employing authentication functionality, which forms part of a Bluetooth communication protocol.

[**0312**] It is appreciated that multi-tier authentication may be provided in the embodiment of **FIG. 12C** by any one or more combinations of the authentication devices and/or functionalities described hereinabove.

[**0313**] Reference is now made to **FIGS. 15A, 15B, 15C, 15D** and **15E**, which are simplified flow charts of methods for obtaining authentication information for five different types of authentication devices.

[**0314**] **FIG. 15A** illustrates methods for obtaining authentication information suitable for a personal digital assistant. As seen in **FIG. 15A** depending on the facilities available in or in association with the personal digital assistant, one of the following authentication functionalities which require obtaining authentication information may be selected:

[**0315**] biometric utilizing fingerprint recognition;

[**0316**] biometric utilizing facial recognition;

[**0317**] password based; and

[**0318**] cryptographic key based.

[**0319**] If the biometric authentication functionality utilizing fingerprint recognition is selected, the personal digital assistant captures the user's fingerprint data.

[**0320**] If the biometric authentication functionality utilizing facial recognition is selected, the personal digital assistant captures the user's facial features.

[**0321**] If the password based authentication functionality is selected, the personal digital assistant captures the user password input.

[**0322**] If the cryptographic key based authentication functionality selected, the personal digital assistant employs a cryptographic key typically stored in its memory.

[**0323**] **FIG. 15B** illustrates methods for obtaining authentication information suitable for a wireless smart card. As seen in **FIG. 15B** depending on the facilities available in or in association with the wireless smart card, one of the following authentication functionalities which require obtaining authentication information may be selected:

[**0324**] cryptographic key based.

[**0325**] If the cryptographic key based authentication functionality selected, the wireless smart card employs a cryptographic key typically stored in its memory.

[**0326**] **FIG. 15C** illustrates methods for obtaining authentication information suitable for a cellular phone. As seen in **FIG. 15C** depending on the facilities available in or in association with the cellular phone, one of the following authentication functionalities which require obtaining authentication information may be selected:

[**0327**] biometric utilizing fingerprint recognition;

[**0328**] biometric utilizing facial recognition;

[**0329**] password based; and

[**0330**] cryptographic key based.

[**0331**] If the biometric authentication functionality utilizing fingerprint recognition is selected, the cellular phone captures the user's fingerprint data.

[**0332**] If the biometric authentication functionality utilizing facial recognition is selected, the cellular phone captures the user's facial features.

[**0333**] If the password based authentication functionality is selected, the cellular phone captures the user password input.

[**0334**] If the cryptographic key based authentication functionality selected, the cellular phone employs a cryptographic key typically stored in its memory.

[**0335**] **FIG. 15D** illustrates methods for obtaining authentication information suitable for an electronic wallet. As seen in **FIG. 15D** depending on the facilities available in or in association with the electronic wallet, one of the following authentication functionalities which require obtaining authentication information may be selected:

[**0336**] cryptographic key based.

[**0337**] If the cryptographic key based authentication functionality selected, the electronic wallet employs a cryptographic key typically stored in its memory.

[**0338**] **FIG. 15E** illustrates methods for obtaining authentication information suitable for a PC. As seen in **FIG. 15E** depending on the facilities available in or in association with

the PC, one of the following authentication functionalities which require obtaining authentication information may be selected:

[0339] biometric utilizing fingerprint recognition;

[0340] biometric utilizing facial recognition;

[0341] password based;

[0342] cryptographic utilizing a memory based key;

[0343] cryptographic utilizing a USB toke n based key;

[0344] cryptographic utilizing a smart card based key; and

[0345] cryptographic utilizing a diskette based key.

[0346] If the biometric authentication functionality utilizing fingerprint recognition is selected, the PC captures the user's fingerprint data.

[0347] If the biometric authentication functionality utilizing facial recognition is selected, the PC captures the user's facial features.

[0348] If the password based authentication functionality is selected, the PC captures the user password input.

[0349] If the cryptographic memory based key authentication functionality is selected, the PC employs a cryptographic key typically stored in its memory.

[0350] If the cryptographic USB token based key authentication functionality is selected, the PC employs a cryptographic key typically stored in the associated USB key.

[0351] If the cryptographic smart card based key authentication functionality is selected, the PC employs a cryptographic key typically stored in the associated smart card.

[0352] If the cryptographic diskette based key authentication functionality is selected, the PC employs a cryptographic key typically stored in the associated key diskette.

[0353] Reference is now made to **FIGS. 16A, 16B** and **16**C, which are simplified flow charts of different multi-tier and non multi-tier authentication using different communication modes between an authenticating device and an authenticator.

[0354] **FIG. 16A** illustrates a non multi-tier authentication using a direct communication mode between an authenticating device and an authenticator. As seen in **FIG. 16A**, an authentication device such as a personal digital assistant, a wireless smart card, a cellular phone, an electronic wallet or a PC negotiates with an authenticator an authentication functionality. Depending on the facilities available in or in association with the authentication device, either a Bluetooth based authentication functionality or non-Bluetooth based authentication functionality may be used.

[0355] If a non-Bluetooth authentication is selected, the authentication device obtains authentication information employing at least one of the functionalities of FIGS. **15A-15**E. The authentication device than communicates authentication information to the authenticator using at least partially the Bluetooth communication protocol. In response to receipt of such information, the authenticator may authenticate the user.

[0356] If the Bluetooth authentication functionality is selected, the authentication device carries out Bluetooth authentication in conjunction with a Bluetooth hub. If the authentication is successful, the authentication device 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.

[0357] 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 authentication device 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 authentication device.

[0358] 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 authentication device.

[0359] **FIG. 16B** illustrates a multi-tier authentication in which an authentication device and an authenticator employ a second device for communication. As seen in **FIG. 16B** an authentication device such as a personal digital assistant, a wireless smart card, a cellular phone, an electronic wallet or a PC negotiates with an authenticator an authentication functionality communicating through said second device, which may be a personal digital assistant, a cellular phone or a PC. Depending on the facilities available in or in association with the authentication device, either a Bluetooth based authentication functionality or non-Bluetooth based authentication functionality may be used.

[0360] If a non-Bluetooth authentication is selected, the authentication device obtains authentication information employing at least one of the functionalities of FIGS. **15A-15**E. The authentication device than communicates authentication information to the authenticator using at least partially the Bluetooth communication protocol and communicating through said second device. In response to receipt of such information, the authenticator may authenticate the user.

[0361] If the Bluetooth authentication functionality is selected, the authentication device carries out Bluetooth authentication in conjunction with a Bluetooth hub. If the authentication is successful, the authentication device requests that the Bluetooth hub send an authentication confirmation to the authenticator communicating through said second device. In response to receipt of the confirmation, the authenticator determines whether the hub, which sent the confirmation, is certified to do so.

[0362] 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 authentication device and the authenticator negotiate the next authentication functionality communicating through said second device and proceed as described hereinabove. If no additional authentication functions are required, the authenticator transmits an authentication confirmation to the authentication device communicating through said second device.

[0363] 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 authentication device communicating through said second device.

[0364] **FIG. 16C** illustrates a multi-tier authentication in which an authentication device employ a proxy to communicate with an authenticator. As seen in **FIG. 16C** an authentication device such as a personal digital assistant, a wireless smart card, a cellular phone, an electronic wallet or a PC negotiates with an authenticator an authentication functionality, said negotiation employing a proxy, which may be a personal digital assistant, a cellular phone or a PC, to communicate with the authenticator. Depending on the facilities available in or in association with the authentication device, either a Bluetooth based authentication functionality or non-Bluetooth based authentication functionality may be used.

[0365] If a non-Bluetooth authentication is selected, the authentication device obtains authentication information employing at least one of the functionalities of FIGS. **15A-15E**. The authentication device transmits authentication information to the proxy. The proxy then transmits the data to the authenticator. One or more of the transmissions use at least partially the Bluetooth communication protocol. In response to receipt of such information, the authenticator may authenticate the user.

[0366] If the Bluetooth authentication functionality is selected, the authentication device carries out Bluetooth authentication in conjunction with a Bluetooth hub. If the authentication is successful, the authentication device requests that the Bluetooth hub send an authentication confirmation to the proxy. The proxy then sends the 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.

[0367] 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 authentication device and the authenticator negotiate the next authentication functionality, said negotiation employing a proxy, and proceed as described hereinabove. If no additional authentication functions are required, the authenticator transmits an authentication confirmation to the proxy. The proxy then transmits the confirmation to the authentication device.

[0368] 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 proxy. The proxy then transmits the non-authentication message to the authentication device.

[0369] Reference is now made to **FIGS. 17A, 17B** and **17C**, which are simplified flow charts of different multi-tier and non multi-tier authentication employing different combinations of authentication devices.

[0370] **FIG. 17A** illustrates a non multi-tier authentication employing a single authentication device. As seen in **FIG. 17A, a** user who requests access to a resource protected by an authenticator may employ an authentication device. The authentication device may employ any one of the functionalities of FIGS. **16A-16C** to perform authentication with the authenticator. When the authentication device receives a confirmation message or a non-authentication message, the authentication device displays a suitable message to the user.

[0371] **FIG. 17B** illustrates a non multi-tier authentication employing multiple authentication devices. As seen in **FIG. 17B, a** user who requests access to a resource protected by an authenticator negotiates with said authenticator an authentication device. The authentication device may employ any one of the functionalities of FIGS. **16A-16C** to perform authentication with the authenticator.

[0372] 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 devices are required. If so, the user and the authenticator negotiate the next authentication device and proceed as described hereinabove. If no additional authentication devices are required, an authentication is granted.

[0373] If authentication of the user and/or device is not successful at any stage, authentication is not granted.

[0374] **FIG. 17C** illustrates a multi-tier authentication employing an enabling device. As seen in **FIG. 17C, a** user who requests access to a resource protected by an authenticator may employ an authentication device. The authenticator may require the authentication device to be enabled for authentication by an enabling device. The enabling device may employ any one of the functionalities of FIGS. **16A-16C** to perform authentication with the authenticator.

[0375] If the enabling device is successfully authenticated, the authentication device may employ any one of the functionalities of FIGS. **16A-16C** to perform authentication with the authenticator. When the authentication device receives a confirmation message or a non-authentication message, the authentication device displays a suitable message to the user.

[0376] It will be appreciated by persons skilled in the art that the present invention is not limited by what has been particularly shown and described hereinabove. Rather the scope of the present invention includes both combinations and subcombinations of the various features described hereinabove as well as variations and modifications which would occur to persons skilled in the art upon reading the specification and which are not in the prior art.

1. A device capable of communicating with a communication network via a Bluetooth communication protocol, said device including at least one authentication functionality, at least part of at least one of which is operative to communicate authentication information via said Bluetooth communication protocol.

2. A device according to claim 1 and wherein said device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

3. A device according to claim 1 and wherein said device is effective to identify said device to an authenticator coupled to said communication network.

4. A device according to claim 1 and wherein said device is effective to identify another device to an authenticator coupled to said communication network.

5. A device according to claim 1 and wherein said device is effective to identify a user to an authenticator coupled to said communication network.

6. A device according to claim 1 and wherein said device is a dedicated authentication device.

7. A device according to claim 6 and wherein said device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

8. A device according to claim 1 and wherein said device includes substantial non-authentication functionality.

9. A device according to claim 8 and wherein said device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

10. A device according to claim 8 and wherein said device comprises a telephone.

11. A device according to claim 8 and wherein said device comprises a PDA.

12. A device according to claim 8 and wherein said device comprises a computer.

13. A device according to claim 8 and wherein said device comprises an electronic wallet.

14. A device according to claim 1 and wherein said at least one authentication functionality comprises plural authentication functionalities.

15. A device according to claim 14 and wherein said device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

16. A device according to claim 14 and wherein said device is a dedicated authentication device.

17. A device according to claim 14 and wherein said device includes substantial non-authentication functionality.

18. A device according to claim 1 and wherein said at least one 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.

19. A device according to claim 1 and wherein said at least one 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.

20. A device according to claim 1 and wherein at least part of said at least one authentication functionality forms part of said Bluetooth communication protocol.

21. A device according to claim 20 and wherein said device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

22. A device according to claim 20 and wherein said device is a dedicated authentication device.

23. A device according to claim 20 and wherein said device includes substantial non-authentication functionality.

24. A device according to claim 20 and wherein said at least one authentication functionality comprises plural authentication functionalities.

25. A device according to claim 24 and wherein said device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

26. A device according to claim 24 and wherein said device is a dedicated authentication device.

27. A device according to claim 24 and wherein said device includes substantial non-authentication functionality.

28. A device according to claim 1 and wherein at least part of said at least one functionality employs a Bluetooth communication protocol.

29. A device according to claim 28 and wherein said device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

30. A device according to claim 28 and wherein said device is a dedicated authentication device.

31. A device according to claim 28 and wherein said device includes substantial non-authentication functionality.

32. A device according to claim 28 and wherein said at least one authentication functionality comprises plural authentication functionalities.

33. A device according to claim 32 and wherein said device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

34. A device according to claim 32 and wherein said device is a dedicated authentication device.

35. A device according to claim 32 and wherein said device includes substantial non-authentication functionality.

36. A device according to claim 28 and wherein at least part of said at least one authentication functionality forms part of said Bluetooth communication protocol.

37. A device according to claim 36 and wherein said device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

38. A device according to claim 36 and wherein said device is a dedicated authentication device.

39. A device according to claim 36 and wherein said device includes substantial non-authentication functionality.

40. A device according to claim 36 and wherein said at least one authentication functionality comprises plural authentication functionalities.

41. A device according to claim 40 and wherein said device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

42. A device according to claim 40 and wherein said device is a dedicated authentication device.

43. A device according to claim 40 and wherein said device includes substantial non-authentication functionality.

44. A device capable of communicating with a communication network via a Bluetooth communication protocol, said device including at least one authentication functionality at least part of at least one of which forms part of said Bluetooth communication protocol.

45. A device according to claim 44 and wherein said device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

46. A device according to claim 44 and wherein said device is effective to identify said device to an authenticator coupled to said communication network.

47. A device according to claim 44 and wherein said device is effective to identify another device to an authenticator coupled to said communication network.

48. A device according to claim 44 and wherein said device is effective to identify a user to an authenticator coupled to said communication network.

49. A device according to claim 44 and wherein said device is a dedicated authentication device.

50. A device according to claim 49 and wherein said device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

51. A device according to claim 44 and wherein said device includes substantial non-authentication functionality.

52. A device according to claim 51 and wherein said device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

53. A device according to claim 51 and wherein said device comprises a telephone.

54. A device according to claim 51 and wherein said device comprises a PDA.

55. A device according to claim 51 and wherein said device comprises a computer.

56. A device according to claim 51 and wherein said device comprises an electronic wallet.

57. A device according to claim 44 and wherein said at least one authentication functionality comprises plural authentication functionalities.

58. A device according to claim 57 and wherein said device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

59. A device according to claim 57 and wherein said device is a dedicated authentication device.

60. A device according to claim 57 and wherein said device includes substantial non-authentication functionality.

61. A device according to claim 44 and wherein said at least one 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.

62. A device according to claim 44 and wherein said at least one 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.

63. A device according to claim 44 and wherein at least part of said at least one functionality employs a Bluetooth communication protocol.

64. A device according to claim 63 and wherein said device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

65. A device according to claim 63 and wherein said device is a dedicated authentication device.

66. A device according to claim 63 and wherein said device includes substantial non-authentication functionality.

67. A device according to claim 63 and wherein said at least one authentication functionality comprises plural authentication functionalities.

68. A device according to claim 67 and wherein said device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

69. A device according to claim 67 and wherein said device is a dedicated authentication device.

70. A device according to claim 67 and wherein said device includes substantial non-authentication functionality.

71. A device capable of communicating with a communication network, said device comprising at least one authentication functionality at least part of at least one of which employs a Bluetooth communication protocol.

72. A device according to claim 71 and wherein said device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

73. A device according to claim 71 and wherein said device is effective to identify said device to an authenticator coupled to said communication network.

74. A device according to claim 71 and wherein said device is effective to identify another device to an authenticator coupled to said communication network.

75. A device according to claim 71 and wherein said device is effective to identify a user to an authenticator coupled to said communication network.

76. A device according to claim 71 and wherein said device is a dedicated authentication device.

77. A device according to claim 76 and wherein said device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

78. A device according to claim 71 and wherein said device includes substantial non-authentication functionality.

79. A device according to claim 78 and wherein said device is effective to identify at least one of said device,

another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

80. A device according to claim 78 and wherein said device comprises a telephone.

81. A device according to claim 78 and wherein said device comprises a PDA.

82. A device according to claim 78 and wherein said device comprises a computer.

83. A device according to claim 78 and wherein said device comprises an electronic wallet.

84. A device according to claim 71 and wherein said at least one authentication functionality comprises plural authentication functionalities.

85. A device according to claim 84 and wherein said device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

86. A device according to claim 84 and wherein said device is a dedicated authentication device.

87. A device according to claim 84 and wherein said device includes substantial non-authentication functionality.

88. A device according to claim 71 and wherein said at least one 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.

89. A device according to claim 71 and wherein said at least one 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.

90. A device according to claim 71 and wherein at least part of said at least one authentication functionality forms part of said Bluetooth communication protocol.

91. A device according to claim 90 and wherein said device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

92. A device according to claim 90 and wherein said device is a dedicated authentication device.

93. A device according to claim 90 and wherein said device includes substantial non-authentication functionality.

94. A device according to claim 90 and wherein said at least one authentication functionality comprises plural authentication functionalities.

95. A device according to claim 94 and wherein said device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

96. A device according to claim 94 and wherein said device is a dedicated authentication device.

97. A device according to claim 94 and wherein said device includes substantial non-authentication functionality.

98. A method for communicating with a communication network via a Bluetooth communication protocol, said method comprising:

at least one authentication functionality, at least part of at least one of which is operative to communicate authentication information via said Bluetooth communication protocol.

99. A method according to claim 98 and wherein said method is effective to identify at least one of a device and a user to at least one authenticator coupled to said communication network.

100. A method according to claim 98 and wherein said method is effective to identify a device to an authenticator coupled to said communication network.

101. A method according to claim 98 and wherein said method is effective to identify a user to an authenticator coupled to said communication network.

102. A method according to claim 98 and wherein said at least one authentication functionality comprises plural authentication functionalities.

103. A method according to claim 102 and wherein said method is effective to identify at least one of a device, and a user to at least one authenticator coupled to said communication network.

104. A method according to claim 98 and wherein said at least one authentication functionality is selected from the following authentication functionalities:

a cryptographic based authentication functionality;

a password based authentication functionality;

a smartcard based authentication functionality;

a token based authentication functionality; and

a biometric based authentication functionality.

105. A method according to claim 98 and wherein said at least one authentication functionality includes at least a plurality of the following authentication functionalities:

a cryptographic based authentication functionality;

a password based authentication functionality;

a smartcard based authentication functionality;

a token based authentication functionality; and

a biometric based authentication functionality.

106. A method according to claim 98 and wherein at least part of said at least one authentication functionality forms part of said Bluetooth communication protocol.

107. A method according to claim 106 and wherein said method is effective to identify at least one of a device and a user to at least one authenticator coupled to said communication network.

108. A method according to claim 106 and wherein said at least one authentication functionality comprises plural authentication functionalities.

109. A method according to claim 108 and wherein said method is effective to identify at least one of a device, and a user to at least one authenticator coupled to said communication network.

110. A method according to claim 98 and wherein at least part of said at least one functionality employs a Bluetooth communication protocol.

111. A method according to claim 110 and wherein said method is effective to identify at least one of a device and a user to at least one authenticator coupled to said communication network.

112. A method according to claim 110 and wherein said at least one authentication functionality comprises plural authentication functionalities.

113. A method according to claim 112 and wherein said method is effective to identify at least one of a device, and a user to at least one authenticator coupled to said communication network.

114. A method according to claim 110 and wherein at least part of said at least one authentication functionality forms part of said Bluetooth communication protocol.

115. A method according to claim 114 and wherein said method is effective to identify at least one of a device and a user to at least one authenticator coupled to said communication network.

116. A method according to claim 114 and wherein said at least one authentication functionality comprises plural authentication functionalities.

117. A method according to claim 116 and wherein said method is effective to identify at least one of a device, and a user to at least one authenticator coupled to said communication network.

118. A method for communicating with a communication network via a Bluetooth communication protocol, said method comprising:

at least one authentication functionality at least part of at least one of which forms part of said Bluetooth communication protocol.

119. A method according to claim 118 and wherein said method is effective to identify at least one of a device and a user to at least one authenticator coupled to said communication network.

120. A method according to claim 118 and wherein said method is effective to identify a device to an authenticator coupled to said communication network.

121. A method according to claim 118 and wherein said method is effective to identify a user to an authenticator coupled to said communication network.

122. A method according to claim 118 and wherein said at least one authentication functionality comprises plural authentication functionalities.

123. A method according to claim 122 and wherein said method is effective to identify at least one of a device, and a user to at least one authenticator coupled to said communication network.

124. A method according to claim 118 and wherein said at least one authentication functionality is selected from the following authentication functionalities:

a cryptographic based authentication functionality;

a password based authentication functionality;

a smartcard based authentication functionality;

a token based authentication functionality; and

a biometric based authentication functionality.

125. A method according to claim 118 and wherein said at least one authentication functionality includes at least a plurality of the following authentication functionalities:

a cryptographic based authentication functionality;

a password based authentication functionality;

a smartcard based authentication functionality;

a token based authentication functionality; and

a biometric based authentication functionality.

126. A method according to claim 118 and wherein at least part of said at least one functionality employs a Bluetooth communication protocol.

127. A method according to claim 126 and wherein said method is effective to identify at least one of a device and a user to at least one authenticator coupled to said communication network.

128. A method according to claim 126 and wherein said at least one authentication functionality comprises plural authentication functionalities.

129. A method according to claim 128 and wherein said method is effective to identify at least one of a device, and a user to at least one authenticator coupled to said communication network.

130. A method for communicating with a communication network via a Bluetooth communication protocol, said method comprising:

at least one authentication functionality at least part of at least one of which employs a Bluetooth communication protocol.

131. A method according to claim 130 and wherein said method is effective to identify at least one of a device and a user to at least one authenticator coupled to said communication network.

132. A method according to claim 130 and wherein said method is effective to identify a device to an authenticator coupled to said communication network.

133. A method according to claim 130 and wherein said method is effective to identify a user to an authenticator coupled to said communication network.

134. A method according to claim 130 and wherein said at least one authentication functionality comprises plural authentication functionalities.

135. A method according to claim 134 and wherein said method is effective to identify at least one of a device, and a user to at least one authenticator coupled to said communication network.

136. A method according to claim 130 and wherein said at least one authentication functionality is selected from the following authentication functionalities:

a cryptographic based authentication functionality;

a password based authentication functionality;

a smartcard based authentication functionality;

a token based authentication functionality; and

a biometric based authentication functionality.

137. A method according to claim 130 and wherein said at least one authentication functionality includes at least a plurality of the following authentication functionalities:

a cryptographic based authentication functionality;

a password based authentication functionality;

a smartcard based authentication functionality;

a token based authentication functionality; and

a biometric based authentication functionality.

137. A method according to claim 130 and wherein at least part of said at least one authentication functionality forms part of said Bluetooth communication protocol.

138. A method according to claim 137 and wherein said method is effective to identify at least one of a device and a user to at least one authenticator coupled to said communication network.

139. A method according to claim 137 and wherein said at least one authentication functionality comprises plural authentication functionalities.

140. A method according to claim 139 and wherein said method is effective to identify at least one of a device, and a user to at least one authenticator coupled to said communication network.

141. A system comprising:

a communication network;

at least one authenticator; and

at least one device capable of communicating with said at least one authenticator through said communication network via a Bluetooth communication protocol, said at least one device including at least one authentication functionality, at least part of at least one of which is operative to communicate authentication information via said Bluetooth communication protocol to said at least one authenticator.

142. A system according to claim 141 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

143. A system according to claim 141 and wherein said at least one device is effective to identify said device to an authenticator coupled to said communication network.

144. A system according to claim 141 and wherein said at least one device is effective to identify another device to an authenticator coupled to said communication network.

145. A system according to claim 141 and wherein said at least one device is effective to identify a user to an authenticator coupled to said communication network.

146. A system according to claim 141 and wherein said at least one device is a dedicated authentication device.

147. A system according to claim 146 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

148. A system according to claim 141 and wherein said at least one device includes substantial non-authentication functionality.

149. A system according to claim 148 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

150. A system according to claim 148 and wherein said at least one device comprises a telephone.

151. A system according to claim 148 and wherein said at least one device comprises a PDA.

152. A system according to claim 148 and wherein said at least one device comprises a computer.

153. A system according to claim 148 and wherein said at least one device comprises an electronic wallet.

154. A system according to claim 141 and wherein said at least one authentication functionality comprises plural authentication functionalities.

155. A system according to claim 154 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

156. A system according to claim 154 and wherein said at least one device is a dedicated authentication device.

157. A system according to claim 154 and wherein said at least one device includes substantial non-authentication functionality.

158. A system according to claim 141 and wherein said at least one 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.

159. A system according to claim 141 and wherein said at least one 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.

160. A system according to claim 141 and wherein at least part of said at least one authentication functionality forms part of said Bluetooth communication protocol.

161. A system according to claim 160 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

162. A system according to claim 160 and wherein said at least one device is a dedicated authentication device.

163. A system according to claim 160 and wherein said at least one device includes substantial non-authentication functionality.

164. A system according to claim 160 and wherein said at least one authentication functionality comprises plural authentication functionalities.

165. A system according to claim 164 and wherein said at least one device is effective to identify at least one of said

device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

166. A system according to claim 164 and wherein said at least one device is a dedicated authentication device.

167. A system according to claim 164 and wherein said at least one device includes substantial non-authentication functionality.

168. A system according to claim 141 and wherein at least part of said at least one functionality employs a Bluetooth communication protocol.

169. A system according to claim 168 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

170. A system according to claim 168 and wherein said at least one device is a dedicated authentication device.

171. A system according to claim 168 and wherein said at least one device includes substantial non-authentication functionality.

172. A system according to claim 168 and wherein said at least one authentication functionality comprises plural authentication functionalities.

173. A system according to claim 172 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

174. A system according to claim 172 and wherein said at least one device is a dedicated authentication device.

175. A system according to claim 172 and wherein said at least one device includes substantial non-authentication functionality.

176. A system according to claim 168 and wherein at least part of said at least one authentication functionality forms part of said Bluetooth communication protocol.

177. A system according to claim 176 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

178. A system according to claim 176 and wherein said at least one device is a dedicated authentication device.

179. A system according to claim 176 and wherein said at least one device includes substantial non-authentication functionality.

180. A system according to claim 176 and wherein said at least one authentication functionality comprises plural authentication functionalities.

181. A system according to claim 180 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

182. A system according to claim 180 and wherein said at least one device is a dedicated authentication device.

183. A system according to claim 180 and wherein said at least one device includes substantial non-authentication functionality.

184. A system comprising:

a communication network;

at least one authenticator; and

at least one device capable of communicating with a communication network via a Bluetooth communication protocol, said device including at least one authentication functionality at least part of at least one of which forms part of said Bluetooth communication protocol.

185. A system according to claim 184 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

186. A system according to claim 184 and wherein said at least one device is effective to identify said device to an authenticator coupled to said communication network.

187. A system according to claim 184 and wherein said at least one device is effective to identify another device to an authenticator coupled to said communication network.

188. A system according to claim 184 and wherein said at least one device is effective to identify a user to an authenticator coupled to said communication network.

189. A system according to claim 184 and wherein said at least one device is a dedicated authentication device.

190. A system according to claim 189 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

191. A system according to claim 184 and wherein said at least one device includes substantial non-authentication functionality.

192. A system according to claim 191 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

193. A system according to claim 191 and wherein said at least one device comprises a telephone.

194. A system according to claim 191 and wherein said at least one device comprises a PDA.

195. A system according to claim 191 and wherein said at least one device comprises a computer.

196. A system according to claim 191 and wherein said at least one device comprises an electronic wallet.

197. A system according to claim 184 and wherein said at least one authentication functionality comprises plural authentication functionalities.

198. A system according to claim 197 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

199. A system according to claim 197 and wherein said at least one device is a dedicated authentication device.

200. A system according to claim 197 and wherein said at least one device includes substantial non-authentication functionality.

201. A system according to claim 184 and wherein said at least one 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.

202. A system according to claim 184 and wherein said at least one 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.

203. A system according to claim 184 and wherein at least part of said at least one functionality employs a Bluetooth communication protocol.

204. A system according to claim 203 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

205. A system according to claim 203 and wherein said at least one device is a dedicated authentication device.

206. A system according to claim 203 and wherein said at least one device includes substantial non-authentication functionality.

207. A system according to claim 203 and wherein said at least one authentication functionality comprises plural authentication functionalities.

208. A system according to claim 207 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

209. A system according to claim 207 and wherein said at least one device is a dedicated authentication device.

210. A system according to claim 207 and wherein said at least one device includes substantial non-authentication functionality.

211. A system comprising:

a communication network;

at least one authenticator; and

at least one device capable of communicating with a communication network, said device comprising at least one authentication functionality at least part of at least one of which employs a Bluetooth communication protocol.

212. A system according to claim 211 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

213. A system according to claim 211 and wherein said at least one device is effective to identify said device to an authenticator coupled to said communication network.

214. A system according to claim 211 and wherein said at least one device is effective to identify another device to an authenticator coupled to said communication network.

215. A system according to claim 211 and wherein said at least one device is effective to identify a user to an authenticator coupled to said communication network.

216. A system according to claim 211 and wherein said at least one device is a dedicated authentication device.

217. A system according to claim 216 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

218. A system according to claim 211 and wherein said at least one device includes substantial non-authentication functionality.

219. A system according to claim 218 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

220. A system according to claim 218 and wherein said at least one device comprises a telephone.

221. A system according to claim 218 and wherein said at least one device comprises a PDA.

222. A system according to claim 218 and wherein said at least one device comprises a computer.

223. A system according to claim 218 and wherein said at least one device comprises an electronic wallet.

224. A system according to claim 211 and wherein said at least one authentication functionality comprises plural authentication functionalities.

225. A system according to claim 224 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

226. A system according to claim 224 and wherein said at least one device is a dedicated authentication device.

227. A system according to claim 224 and wherein said at least one device includes substantial non-authentication functionality.

228. A system according to claim 211 and wherein said at least one 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.

229. A system according to claim 211 and wherein said at least one 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.

230. A system according to claim 211 and wherein at least part of said at least one authentication functionality forms part of said Bluetooth communication protocol.

231. A system according to claim 230 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

232. A system according to claim 230 and wherein said at least one device is a dedicated authentication device.

233. A system according to claim 230 and wherein said at least one device includes substantial non-authentication functionality.

234. A system according to claim 230 and wherein said at least one authentication functionality comprises plural authentication functionalities.

235. A system according to claim 234 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

236. A system according to claim 234 and wherein said at least one device is a dedicated authentication device.

237. A system according to claim 234 and wherein said at least one device includes substantial non-authentication functionality.

238. A system comprising:

at least one authenticator; and

at least one device capable of communicating with said at least one authenticator via a Bluetooth communication protocol, said at least one device including at least one authentication functionality, at least part of at least one of which is operative to communicate authentication information via said Bluetooth communication protocol to said at least one authenticator.

239. A system according to claim 238 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

240. A system according to claim 238 and wherein said at least one device is effective to identify said device to an authenticator coupled to said communication network.

241. A system according to claim 238 and wherein said at least one device is effective to identify another device to an authenticator coupled to said communication network.

242. A system according to claim 238 and wherein said at least one device is effective to identify a user to an authenticator coupled to said communication network.

243. A system according to claim 238 and wherein said at least one device is a dedicated authentication device.

244. A system according to claim 243 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

245. A system according to claim 238 and wherein said at least one device includes substantial non-authentication functionality.

246. A system according to claim 245 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

247. A system according to claim 245 and wherein said at least one device comprises a telephone.

248. A system according to claim 245 and wherein said at least one device comprises a PDA.

249. A system according to claim 245 and wherein said at least one device comprises a computer.

250. A system according to claim 245 and wherein said at least one device comprises an electronic wallet.

251. A system according to claim 238 and wherein said at least one authentication functionality comprises plural authentication functionalities.

252. A system according to claim 251 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

253. A system according to claim 251 and wherein said at least one device is a dedicated authentication device.

254. A system according to claim 251 and wherein said at least one device includes substantial non-authentication functionality.

255. A system according to claim 238 and wherein said at least one 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.

256. A system according to claim 238 and wherein said at least one 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.

257. A system according to claim 238 and wherein at least part of said at least one authentication functionality forms part of said Bluetooth communication protocol.

258. A system according to claim 257 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

259. A system according to claim 257 and wherein said at least one device is a dedicated authentication device.

260. A system according to claim 257 and wherein said at least one device includes substantial non-authentication functionality.

261. A system according to claim 257 and wherein said at least one authentication functionality comprises plural authentication functionalities.

262. A system according to claim 261 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

263. A system according to claim 261 and wherein said at least one device is a dedicated authentication device.

264. A system according to claim 261 and wherein said at least one device includes substantial non-authentication functionality.

265. A system according to claim 238 and wherein at least part of said at least one functionality employs a Bluetooth communication protocol.

266. A system according to claim 265 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

267. A system according to claim 265 and wherein said at least one device is a dedicated authentication device.

268. A system according to claim 265 and wherein said at least one device includes substantial non-authentication functionality.

269. A system according to claim 265 and wherein said at least one authentication functionality comprises plural authentication functionalities.

270. A system according to claim 269 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

271. A system according to claim 269 and wherein said at least one device is a dedicated authentication device.

272. A system according to claim 269 and wherein said at least one device includes substantial non-authentication functionality.

273. A system according to claim 265 and wherein at least part of said at least one authentication functionality forms part of said Bluetooth communication protocol.

274. A system according to claim 273 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

275. A system according to claim 273 and wherein said at least one device is a dedicated authentication device.

276. A system according to claim 273 and wherein said at least one device includes substantial non-authentication functionality.

277. A system according to claim 273 and wherein said at least one authentication functionality comprises plural authentication functionalities.

278. A system according to claim 277 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

279. A system according to claim 277 and wherein said at least one device is a dedicated authentication device.

280. A system according to claim 277 and wherein said at least one device includes substantial non-authentication functionality.

281. A system comprising:

at least one authenticator; and

at least one device capable of communicating with said at least one authenticator via a Bluetooth communication protocol, said at least one device including at least one authentication functionality, at least part of at least one of which forms part of said Bluetooth communication protocol.

282. A system according to claim 281 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

283. A system according to claim 281 and wherein said at least one device is effective to identify said device to an authenticator coupled to said communication network.

284. A system according to claim 281 and wherein said at least one device is effective to identify another device to an authenticator coupled to said communication network.

285. A system according to claim 281 and wherein said at least one device is effective to identify a user to an authenticator coupled to said communication network.

286. A system according to claim 281 and wherein said at least one device is a dedicated authentication device.

287. A system according to claim 286 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

288. A system according to claim 281 and wherein said at least one device includes substantial non-authentication functionality.

289. A system according to claim 288 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

290. A system according to claim 288 and wherein said at least one device comprises a telephone.

291. A system according to claim 288 and wherein said at least one device comprises a PDA.

292. A system according to claim 288 and wherein said at least one device comprises a computer.

293. A system according to claim 288 and wherein said at least one device comprises an electronic wallet.

294. A system according to claim 281 and wherein said at least one authentication functionality comprises plural authentication functionalities.

295. A system according to claim 294 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

296. A system according to claim 294 and wherein said at least one device is a dedicated authentication device.

297. A system according to claim 294 and wherein said at least one device includes substantial non-authentication functionality.

298. A system according to claim 281 and wherein said at least one 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.

299. A system according to claim 281 and wherein said at least one 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.

300. A system according to claim 281 and wherein at least part of said at least one functionality employs a Bluetooth communication protocol.

301. A system according to claim 300 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

302. A system according to claim 300 and wherein said at least one device is a dedicated authentication device.

303. A system according to claim 300 and wherein said at least one device includes substantial non-authentication functionality.

304. A system according to claim 300 and wherein said at least one authentication functionality comprises plural authentication functionalities.

305. A system according to claim 304 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

306. A system according to claim 304 and wherein said at least one device is a dedicated authentication device.

307. A system according to claim 304 and wherein said at least one device includes substantial non-authentication functionality.

308. A system comprising:

at least one authenticator; and

at least one device capable of communicating with said at least one authenticator via a Bluetooth communication protocol, said at least one device including at least one authentication functionality at least part of at least one of which employs a Bluetooth communication protocol.

309. A system according to claim 308 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

310. A system according to claim 308 and wherein said at least one device is effective to identify said device to an authenticator coupled to said communication network.

311. A system according to claim 308 and wherein said at least one device is effective to identify another device to an authenticator coupled to said communication network.

312. A system according to claim 308 and wherein said at least one device is effective to identify a user to an authenticator coupled to said communication network.

313. A system according to claim 308 and wherein said at least one device is a dedicated authentication device.

314. A system according to claim 313 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

315. A system according to claim 308 and wherein said at least one device includes substantial non-authentication functionality.

316. A system according to claim 315 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

317. A system according to claim 315 and wherein said at least one device comprises a telephone.

318. A system according to claim 315 and wherein said at least one device comprises a PDA.

319. A system according to claim 315 and wherein said at least one device comprises a computer.

320. A system according to claim 315 and wherein said at least one device comprises an electronic wallet.

321. A system according to claim 308 and wherein said at least one authentication functionality comprises plural authentication functionalities.

322. A system according to claim 321 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

323. A system according to claim 312 and wherein said at least one device is a dedicated authentication device.

324. A system according to claim 321 and wherein said at least one device includes substantial non-authentication functionality.

325. A system according to claim 308 and wherein said at least one 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.

326. A system according to claim 308 and wherein said at least one 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.

327. A system according to claim 308 and wherein at least part of said at least one authentication functionality forms part of said Bluetooth communication protocol.

328. A system according to claim 327 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

329. A system according to claim 327 and wherein said at least one device is a dedicated authentication device.

330. A system according to claim 327 and wherein said at least one device includes substantial non-authentication functionality.

331. A system according to claim 327 and wherein said at least one authentication functionality comprises plural authentication functionalities.

332. A system according to claim 331 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

333. A system according to claim 331 and wherein said at least one device is a dedicated authentication device.

334. A system according to claim 331 and wherein said at least one device includes substantial non-authentication functionality.

335. A system comprising:

a communication network;

at least one authenticator; and

at least one device capable of communicating with said at least one authenticator through said communication network via a Bluetooth communication protocol, said at least one device including at least one multi-tier authentication functionality, at least part of at least one of which is operative to communicate authentication information via said Bluetooth communication protocol to said at least one authenticator.

336. A system according to claim 335 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

337. A system according to claim 335 and wherein said at least one device is effective to identify said device to an authenticator coupled to said communication network.

338. A system according to claim 335 and wherein said at least one device is effective to identify another device to an authenticator coupled to said communication network.

339. A system according to claim 335 and wherein said at least one device is effective to identify a user to an authenticator coupled to said communication network.

340. A system according to claim 335 and wherein said at least one device is a dedicated authentication device.

341. A system according to claim 340 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

342. A system according to claim 335 and wherein said at least one device includes substantial non-authentication functionality.

343. A system according to claim 342 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

344. A system according to claim 342 and wherein said at least one device comprises a telephone.

345. A system according to claim 342 and wherein said at least one device comprises a PDA.

346. A system according to claim 342 and wherein said at least one device comprises a computer.

347. A system according to claim 342 and wherein said at least one device comprises an electronic wallet.

348. A system according to claim 335 and wherein said at least one authentication functionality comprises plural authentication functionalities.

349. A system according to claim 348 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

350. A system according to claim 348 and wherein said at least one device is a dedicated authentication device.

351. A system according to claim 348 and wherein said at least one device includes substantial non-authentication functionality.

352. A system according to claim 335 and wherein said at least one 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.

353. A system according to claim 335 and wherein said at least one 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.

354. A system according to claim 335 and wherein at least part of said at least one authentication functionality forms part of said Bluetooth communication protocol.

355. A system according to claim 354 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

356. A system according to claim 354 and wherein said at least one device is a dedicated authentication device.

357. A system according to claim 354 and wherein said at least one device includes substantial non-authentication functionality.

358. A system according to claim 354 and wherein said at least one authentication functionality comprises plural authentication functionalities.

359. A system according to claim 358 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

360. A system according to claim 358 and wherein said at least one device is a dedicated authentication device.

361. A system according to claim 358 and wherein said at least one device includes substantial non-authentication functionality.

362. A system according to claim 335 and wherein at least part of said at least one functionality employs a Bluetooth communication protocol.

363. A system according to claim 362 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

364. A system according to claim 362 and wherein said at least one device is a dedicated authentication device.

365. A system according to claim 362 and wherein said at least one device includes substantial non-authentication functionality.

366. A system according to claim 362 and wherein said at least one authentication functionality comprises plural authentication functionalities.

367. A system according to claim 366 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

368. A system according to claim 366 and wherein said at least one device is a dedicated authentication device.

369. A system according to claim 366 and wherein said at least one device includes substantial non-authentication functionality.

370. A system according to claim 265 and wherein at least part of said at least one authentication functionality forms part of said Bluetooth communication protocol.

371. A system according to claim 370 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

372. A system according to claim 370 and wherein said at least one device is a dedicated authentication device.

373. A system according to claim 370 and wherein said at least one device includes substantial non-authentication functionality.

374. A system according to claim 370 and wherein said at least one authentication functionality comprises plural authentication functionalities.

375. A system according to claim 374 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

376. A system according to claim 374 and wherein said at least one device is a dedicated authentication device.

377. A system according to claim 374 and wherein said at least one device includes substantial non-authentication functionality.

378. A system comprising:

a communication network;

at least one authenticator; and

at least one device capable of communicating with said at least one authenticator through said communication network via a Bluetooth communication protocol, said at least one device including at least one multi-tier authentication functionality at least part of at least one of which forms part of said Bluetooth communication protocol.

379. A system according to claim 378 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

380. A system according to claim 378 and wherein said at least one device is effective to identify said device to an authenticator coupled to said communication network.

381. A system according to claim 378 and wherein said at least one device is effective to identify another device to an authenticator coupled to said communication network.

382. A system according to claim 378 and wherein said at least one device is effective to identify a user to an authenticator coupled to said communication network.

383. A system according to claim 378 and wherein said at least one device is a dedicated authentication device.

384. A system according to claim 383 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

385. A system according to claim 378 and wherein said at least one device includes substantial non-authentication functionality.

386. A system according to claim 385 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

387. A system according to claim 385 and wherein said at least one device comprises a telephone.

388. A system according to claim 385 and wherein said at least one device comprises a PDA.

389. A system according to claim 385 and wherein said at least one device comprises a computer.

390. A system according to claim 385 and wherein said at least one device comprises an electronic wallet.

391. A system according to claim 378 and wherein said at least one authentication functionality comprises plural authentication functionalities.

392. A system according to claim 391 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

393. A system according to claim 391 and wherein said at least one device is a dedicated authentication device.

394. A system according to claim 391 and wherein said at least one device includes substantial non-authentication functionality.

395. A system according to claim 378 and wherein said at least one 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.

396. A system according to claim 378 and wherein said at least one 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.

397. A system according to claim 378 and wherein at least part of said at least one functionality employs a Bluetooth communication protocol.

398. A system according to claim 397 and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

399. A system according to claim 397 and wherein said at least one device is a dedicated authentication device.

400. A system according to claim 397 and wherein said at least one device includes substantial non-authentication functionality.

401. A system according to claim 397 and wherein said at least one authentication functionality comprises plural authentication functionalities.

402. A system according to claim **401** and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

403. A system according to claim **401** and wherein said at least one device is a dedicated authentication device.

404. A system according to claim **401** and wherein said at least one device includes substantial non-authentication functionality.

405. A system comprising:

a communication network;

at least one authenticator; and

at least one device capable of communicating with said at least one authenticator through said communication network via a Bluetooth communication protocol, said at least one device including at least one multi-tier authentication functionality at least part of at least one of which employs a Bluetooth communication protocol.

406. A system according to claim **405** and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

407. A system according to claim **405** and wherein said at least one device is effective to identify said device to an authenticator coupled to said communication network.

408. A system according to claim **405** and wherein said at least one device is effective to identify another device to an authenticator coupled to said communication network.

409. A system according to claim **405** and wherein said at least one device is effective to identify a user to an authenticator coupled to said communication network.

410. A system according to claim **405** and wherein said at least one device is a dedicated authentication device.

411. A system according to claim **410** and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

412. A system according to claim **405** and wherein said at least one device includes substantial non-authentication functionality.

413. A system according to claim **412** and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

414. A system according to claim **412** and wherein said at least one device comprises a telephone.

415. A system according to claim **412** and wherein said at least one device comprises a PDA.

416. A system according to claim **412** and wherein said at least one device comprises a computer.

417. A system according to claim **412** and wherein said at least one device comprises an electronic wallet.

418. A system according to claim **405** and wherein said at least one authentication functionality comprises plural authentication functionalities.

419. A system according to claim **418** and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

420. A system according to claim **409** and wherein said at least one device is a dedicated authentication device.

421. A system according to claim **418** and wherein said at least one device includes substantial non-authentication functionality.

422. A system according to claim **405** and wherein said at least one 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.

423. A system according to claim **405** and wherein said at least one 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.

424. A system according to claim **405** and wherein at least part of said at least one authentication functionality forms part of said Bluetooth communication protocol.

425. A system according to claim **424** and wherein said at least one device is effective to identify at least one of said device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

426. A system according to claim **424** and wherein said at least one device is a dedicated authentication device.

427. A system according to claim **424** and wherein said at least one device includes substantial non-authentication functionality.

428. A system according to claim **424** and wherein said at least one authentication functionality comprises plural authentication functionalities.

429. A system according to claim **428** and wherein said at least one device is effective to identify at least one of said

device, another device and a user of said device or of said another device to at least one authenticator coupled to said communication network.

430. A system according to claim **428** and wherein said at least one device is a dedicated authentication device.

431. A system according to claim **428** and wherein said at least one device includes substantial non-authentication functionality.

432. A system according to claim 335 and wherein said at least one multiple-tier authentication functionality is operative to enable a first device to communicate to said at least one authenticator, authentication information provided by at least one second device.

433. A system according to claim 378 and wherein said at least one multiple-tier authentication functionality is operative to enable a first device to communicate to said at least one authenticator, authentication information provided by at least one second device.

434. A system according to claim **405** and wherein said at least one multiple-tier authentication functionality is operative to enable a first device to communicate to said at least one authenticator, authentication information provided by at least one second device.

435. A system according to claim 335 and wherein said at least one multiple-tier authentication functionality is operative to enable a first device to be employed as an authentication proxy when suitably enabled by at least one second device.

436. A system according to claim 378 and wherein said at least one multiple-tier authentication functionality is operative to enable a first device to be employed as an authentication proxy when suitably enabled by at least one second device.

437. A system according to claim **405** and wherein said at least one multiple-tier authentication functionality is operative to enable a first device to be employed as an authentication proxy when suitably enabled by at least one second device.

438. A system according to claim 335 and wherein said at least one multiple-tier authentication functionality is operative to enable an authenticator to require authentication from another device.

439. A system according to claim 378 and wherein said at least one multiple-tier authentication functionality is operative to enable an authenticator to require authentication from another device.

440. A system according to claim **405** and wherein said at least one multiple-tier authentication functionality is operative to enable an authenticator to require authentication from another device.

* * * * *