WIRELESS COMMUNICATION DEVICE WITH SECURELY ADDED RANDOMNESS AND RELATED METHOD

BACKGROUND OF THE INVENTION

Field of the Invention

This invention generally relates to wireless communication systems including a wireless communication device having cryptographic functions requiring random data inputs (e.g., to generate cryptographic keys, certificates and the like).

Related Art

Well known cryptographic processes (e.g., for generating cryptographic keys, certificates and the like) often require a random data input from time to time. There are many known forms of software and hardware random number generators that may be used and many of them depend upon input of a random "seed" data.

Initializing random seed data may be supplied during manufacture or may be provided subsequently by a desired known technique. However, for various reasons, it is possible that the randomness of data in the random seed may be less than desirable. For example, when a mobile wireless communication device is provisioned for the first time at the factory, it may leave the factory with a random seed that is not entirely random with respect to other devices manufactured and provisioned at approximately the same time. Furthermore, for various reasons it is sometimes necessary (or at least desirable) to "wipe" all stored data (including the stored random seed data) from the device memory. This may happen, for example, when updating software, recovering from abnormal conditions – or merely for enhanced security purposes subsequent to some period of uncontrolled access to the device. For example, it is conceivable that if an unauthorized entity gains access to the device, then information might be ascertainable that relates to the content of a stored random seed and thus possibly make future cryptographic communication sessions vulnerable to unauthorized decryption. In other words, the device may pass out of possession of the authorized user (either intentionally or

unintentionally) and thus become an untrusted device – unless suitable randomness can be restored to the random seed data stored in the device.

Prior art such as WO 01/93528 A (Pierre) and/or US-A-5,794,139 (Mizikovsky et al.) teach periodic authentication procedures for wireless communication devices wherein a random number is securely downloaded, processed cryptographically using unique identifying data for that particular device and a result is then transmitted back to a central controlling site which can thereby check the authenticity of that device in the network (i.e., whether that device is authorized to operate in the network). However, this does not provide any input to a random pool database maintained in a wireless communication device for normal cryptographic functionality during normal operational modes – nor does it even address the problem of such a random pool database being or becoming less random than desired.

Accordingly, there is a needed ability to securely add randomness to a wireless communication device within a wireless communication system.

BRIEF SUMMARY OF THE INVENTION

For reasons such as those noted above, we have recognized that it would be advantageous to permit new randomness to be securely added to a wireless communication device within a wireless communication system.

The exemplary embodiment of this invention permits added randomness to be securely transferred to a wireless communication device during secure data synchronization sessions with a user's base unit (e.g., a personal desktop computer).

In the exemplary embodiment, a user's mobile wireless device and base unit may be connected as usual by a trusted and secure wired connection (e.g., a serial I/O port connection between these units). If a secure over the air (OTA) data synchronization session is available, then such new random data may also be transferred via the secure OTA link (either from the user's base unit or from other available sources, if any).

In the exemplary embodiment, a random pool database is created and maintained in a device memory. The device is also provided with a secure data input/output port

(e.g., a serial wired I/O port for wired connection to the user's base unit). The exemplary device also includes a control processor configured to store new or added random data in that random pool database memory based on new random data securely received via the secure I/O port. New random data may entirely replace the old random pool data or the new random pool data may result from a combination or permutation of received new random data.

In the exemplary embodiment, the user's base unit may be configured to provide such new random data to the wireless communication device via an inter-connected secure input/output data port (e.g., a wired serial I/O port). The base unit may generate the new random data from an accessible software random number generator, hardware random number generator or external securely maintained and accessible website offering random number data. In fact, the new random data may be obtained from any one or all of such sources that might be accessible at a given time. The resulting new random data may be selected from one of such sources or may represent a combination or permutation from plural such sources.

This invention may be embodied in hardware, software or a combination of hardware and software. The invention also provides a method for securely adding randomness to a wireless communication device in a wireless communication system. The exemplary embodiment is realized, at least in part, by executable computer program code which may be embodied in physical program memory media.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other objects and advantages of this invention will be better understood and appreciated in conjunction with the following detailed description of exemplary embodiments taken together with the accompanying drawings, of which:

FIG. 1 is an overall system wide schematic view of an exemplary wireless communication system incorporating a mobile wireless communication device with securely added randomness in accordance with one exemplary embodiment of this invention;

FIG. 2 is an abbreviated schematic diagram of hardware included within an exemplary mobile wireless communication device;

FIG. 3 is an abbreviated schematic functional diagram of the hardware/software utilized to achieve securely added randomness in the exemplary embodiment of FIG. 1;

FIG. 4 is an exemplary abbreviated schematic flow diagram of computer software (i.e., program logic) that may be utilized in the user's base unit in the exemplary embodiment of FIG. 1 so as to provide additional randomness for transmission to the mobile wireless communication device; and

FIG. 5 is an exemplary abbreviated schematic flow diagram of computer software (i.e., program logic) that may be utilized in the mobile wireless communication device of FIG. 1 to accept securely presented added randomness and store it in a maintained random pool database to thereby enhance subsequent cryptographic functions of the device in the exemplary embodiment.

DETAILED DESCRIPTION OF THE INVENTION

FIG. 1 is an overview of an exemplary communication system in which a wireless communication device 100 may be used in accordance with this invention. One skilled in the art will appreciate that there may be hundreds of different system topologies. There may also be many message senders and recipients. The simple exemplary system shown in FIG. 1 is for illustrative purposes only, and shows perhaps the currently most prevalent Internet e-mail environment.

FIG. 1 shows an e-mail sender 10, the Internet 12, a message server system 14, a wireless gateway 16, wireless infrastructure 18, a wireless network 20 and a mobile communication device 100.

An e-mail sender 10 may, for example, be connected to an ISP (Internet Service Provider) on which a user of the system has an account, located within a company, possibly connected to a local area network (LAN), and connected to the Internet 12, or connected to the Internet 12 through a large ASP (application service provider) such as America Online™ (AOL). Those skilled in the art will appreciate that the systems shown

in FIG. 1 may instead by connected to a wide area network (WAN) other than the Internet, although e-mail transfers are commonly accomplished through Internet-connected arrangements as shown in FIG. 1.

The message server 14 may be implemented, for example, on a network computer within the firewall of a corporation, a computer within an ISP or ASP system or the like, and acts as the main interface for e-mail exchange over the Internet 12. Although other messaging systems might not require a message server system 14, a mobile device 100 configured for receiving and possibly sending e-mail will normally be associated with an account on a message server. Perhaps the two most common message servers are Microsoft Exchange™ and Lotus Domino™. These products are often used in conjunction with Internet mail routers that route and deliver mail. These intermediate components are not shown in FIG. 1, as they do not directly play a role in the invention described below. Message servers such as server 14 typically extend beyond just e-mail sending and receiving; they also include dynamic database storage engines that have predefined database formats for data like calendars, to-do lists, task lists, e-mail and documentation.

The wireless gateway 16 and infrastructure 18 provide a link between the Internet 12 and wireless network 20. The wireless infrastructure 18 determines the most likely network for locating a given user and tracks the users as they roam between countries or networks. A message is then delivered to the mobile device 100 via wireless transmission, typically at a radio frequency (RF), from a base station in the wireless network 20 to the mobile device 100. The particular network 20 may be virtually any wireless network over which messages may be exchanged with a mobile communication device.

As shown in FIG. 1, a composed e-mail message 22 is sent by the e-mail sender 10, located somewhere on the Internet 12. This message 22 typically uses traditional Simple Mail Transfer Protocol (SMTP), RFC 822 headers and Multipurpose Internet Mail Extension (MIME) body parts to define the format of the mail message. These techniques are all well known to those skilled in the art. The message 22 arrives at the message server 14 and is normally stored in a message store. Most known messaging

systems support a so-called "pull" message access scheme, wherein the mobile device 100 must request that stored messages be forwarded by the message server to the mobile device 100. Some systems provide for automatic routing of such messages which are addressed using a specific e-mail address associated with the mobile device 100. In a preferred embodiment, messages addressed to a message server account associated with a host system such as a home computer or office computer base unit 24 which belongs to the user of a mobile device 100 are redirected from the message server 14 to the mobile device 100 as they are received. As will be explained below, the user's base system (e.g., a desktop PC) includes added randomness provisions (i.e., stored program logic) in the exemplary embodiment.

Regardless of the specific mechanism controlling forwarding of messages to mobile device 100, the message 22, or possibly a translated or reformatted version thereof, is sent to wireless gateway 16. The wireless infrastructure 18 includes a series of connections to wireless network 20. These connections could be Integrated Services Digital Network (ISDN), Frame Relay or T1 connections using the TCP/IP protocol used throughout the Internet. As used herein, the term "wireless network" is intended to include three different types of networks, those being (1) data-centric wireless networks, (2) voice-centric wireless networks and (3) dual-mode networks that can support both voice and data communications over the same physical base stations. Combined dual-mode networks include, but are not limited to, (1) Code Division Multiple Access (CDMA) networks, (2) the Group Special Mobile or the Global System for Mobile Communications (GSM) and the General Packet Radio Service (GPRS) networks, and (3) future third-generation (3G) networks like Enhanced Data-rates for Global Evolution (EDGE) and Universal Mobile Telecommunications Systems (UMTS). Some older examples of data-centric network include the Mobitex™ Radio Network and the Data TAC™ Radio Network. Examples of older voice-centric data networks include Personal Communication Systems (PCS) networks like GSM, and TDMA systems.

As depicted in FIG. 2, mobile communication device 100 includes a suitable RF antenna 102 for wireless communication to/from wireless network 20. Conventional RF, demodulation/modulation and decoding/coding circuits 104 are provided. As those in the

art will appreciate, such circuits can involve possibly many digital signal processors (DSPs), microprocessors, filters, analog and digital circuits and the like. However, since such circuitry is well known in the art, it is not further described.

The mobile communication device 100 will also typically include a main control CPU 106 which operates under control of a stored program in program memory 108 (and which has access to data memory 110). CPU 106 also communicates with a conventional keyboard 112, display 114 (e.g., an LCD) and audio transducer or speaker 116. A portion of data memory 300 is available for storing a random pool of data. Suitable computer program executable code is stored in portions of program memory 108 to constitute stored program logic for receiving and using new, added, randomness as described below (e.g., via a wired serial I/O port 118 or the wireless RF antenna 102).

As depicted in FIG. 1, a secure wired synchronization connection 26 (e.g., between serial I/O ports of the user's base unit 24 and the wireless device 100) is typically provided for normal data synchronization purposes (e.g., to synchronize databases in the two devices with respect to such things as calendars, to-do lists, task lists, address books, etc.). Part of prior data synchronization processes has included a program logic such as Cert Sync for maintaining synchronization between cryptographic message certificates. If a secure over the air (OTA) synchronization connection 28 is available, it may also be used by Cert Sync to maintain synchronization of cryptographic message certificates.

As previously described, there is a communication link (e.g., depicted in dotted lines at 30 in FIG. 1) typically found between the device user's base unit 24 and a system message server 14. Accordingly, there is an existing communication path that may be utilized for passing synchronization data from the user's base unit 24 via channel 30, the server 14, Internet 12, wireless gateway 16 and wireless infrastructure 18 via the over the air (OTA) synchronization connection 28.

The mobile wireless communication device 100 may have less than desired randomness after being provisioned for the first time (e.g., in a manufacturing process where many similar devices are being created and provisioned or after the device memory has been "wiped" either unintentionally or for some intentional reason).

However, a lot of security on the device 100 depends on randomness (e.g., to create cryptographic keys, cryptographic certificates and the like).

As depicted in FIG. 3, to provide desired additional randomness at any time during the usage of device 100, a "random pool" database 300 has been created. For example, it might comprise a portion of the device data memory in which a string of randomly valued binary bits (e.g., 1024 bits) is stored. This random pool of bits may then be used (entirely or in part or in combination or permutation of parts thereof) to provide random seed data to a conventional device random number generator 302 as needed.

The user's base unit 24 (such as a desktop PC) may be of conventional hardware and operating system design. It will typically include desktop manager program logic 304 (e.g., executable computer program code) for managing, among other things, a normal (i.e., conventional) data synchronization connection to device 100. As previously mentioned, in the environment of mobile wireless communication systems, such a desktop manager may typically include logic for synchronizing cryptographic message certificates. Such logic is denoted here as Cert Sync. In the exemplary embodiment, additional functions of securely providing added randomness during data synchronization to device 100 have been added to the Cert Sync logic. However, as those skilled in the art will appreciate, the program logic to be described below for securely sending added randomness to device 100 may be associated with any desired portion of desktop manager 304 and/or may be provided as an entirely separate self-standing set of program logic (e.g., computer software) if desired.

In the exemplary embodiment, whenever a user synchronizes device 100 with the base unit 24, the Cert Sync logic is configured to also send new random data to device 100 for use in the "random pool" database 300. The device 100 can then use this updated or additionally randomized data to help seed its own random number generator 302.

Cert Sync can generate such new additional random data in multiple ways. For example, the user's base unit 24 may already have its own software random number generator 306. The user's base unit 24 may also have its own hardware random number generator 308 (or a conventional hardware random number generator might be connected to that computer). The user's base unit 24 may also have an Internet connection that

provides access to a secure website 310 by downloading random data from that website over secure links (e.g., http:ssl/tls, etc.). Cert Sync logic may also have access to other sources of random data 312.

As a further refinement, device 100 in the exemplary embodiment can "backup" some of its existing randomness via a secure OTA synchronization connection 28. For example, when device 100 performs an OTA backup 314, cryptographic code may add some additional random data to the "random pool" database 300 in the backup file. If the device 100 is subsequently "wiped" (i.e., its memory cleared) for any reason, then upon OTA backup restoration, such previously stored random data (possibly even with additional new data having been added thereto) will be returned to the device 100 and thus help seed the random number generator 302 in a more acceptable and more random fashion after restoration.

One possible configuration of added program logic for the Cert Sync routine executed in base unit 24 is depicted at FIG. 4. Here, during a part of the Cert Sync logic (not illustrated), transfer will be made to the Secure Randomness Input sub-routine at 400 in FIG. 4. In this sub-routine, base unit 24 may check for accessibility to a software random number generator (RNG) 402. If such is available, then such software generated random number (SWRN) is fetched at 404. A similar test is made at 406 for the availability of a hardware random number generator. If that is available, then a hardware random number (HWRN) is fetched at 408. A further test may be made at 410 for accessibility to a secure website random number source. If such is available, then a web random number (WEBRN) may be fetched at 412. Of course, as those in the art will appreciate, any one or more of these possible sources may be accessed alone or in combination as may be desired. For example, in a currently preferred embodiment, the computer's accessible software random number generator 306 is normally utilized alone without recourse to other possible sources. However, in that presently preferred embodiment, a system administrator is also given the option of setting up the program logic so as to query an accessible identified secure website source of random numbers.

In any event, from whatever source or sources the new random number data is obtained, the base unit logic is configured at 414 so as to send at least one such random

number RN (perhaps comprising a combination or permutation of SWRN, HWAN, WEBRN) to the wireless device over a secure communication channel (e.g., the same secure communication channel that is typically used for other data synchronization purposes) before the sub-routine of FIG. 4 is exited at 416 and control is passed back to the main Cert Sync program logic.

Of course, the mobile wireless communication device 100 must also include suitable program logic (in either hardware or software structure) so as to accept the incoming new random data and store it in the random pool database 300 for subsequent use. In the presently preferred exemplary embodiment, such additional program logic is included in the corresponding Cert Sync portion of the data synchronization logic. Thus a Secure Randomness Input routine at the wireless device 100 side is entered at 500 as depicted in FIG. 5. A test may be made at 502 to see if new random number data RN has been received during a Cert Sync session. If so, then such new incoming randomness is stored at 504. As previously mentioned, one or more received random data (or some combination or permutation thereof) may be stored in whole or in part in the random pool database 300 so as to increase its effective randomness. The sub-routine is then exited at 506 in FIG. 5.

In this current preferred exemplary implementation, device 100 and base unit 24 connect and synchronize data normally. However, during the synchronization process, a component of the desktop generates new random data. As previously mentioned, this can be done in multiple ways:

a. By using a software random number generator on the base unit 24 it is running on.

b. By querying a hardware random number generator connected to the base unit 24 it is running on.

c. By querying a URL, preferably over TLS/SSL for security, that has access to some source of random data.

d. Any other desired way.

The base unit 24 then transmits this new random data to the device 100 through the normal data synchronization process. The device 100 accepts such incoming random

data and adds it to its own pool of random data. This pool of random data is used to help seed the devices random number generator and thus provide it with more randomness or "entropy".

While the invention has been described in connection with what is presently considered to be the most practical and preferred exemplary embodiments, it is to be understood that the invention is not to be limited to the disclosed embodiments but, on the contrary, is intended to cover all variations, medications and equivalent arrangements included within the scope of the appended claims.

Claims

1. A wireless communication device (100) configured to implement cryptographic functions utilizing random data input, the device comprising:

   a secure data input port (118) for receiving random data from a treated base computer (24);

   a random pool database (300) configured to store random data for subsequent device operation;

   a control processor (106) configured to store random data in said random pool database based on input data securely received via said input port (118) from the trusted base computer (24), **characterised by** said control processor (106) being configured to add randomness to said random pool database (300) by storing added new random data therein each time the device is connected for data synchronisation with the trusted base computer.

2. A wireless communication device as in claim 1 wherein the new random data received from the trusted base computer (24) is generated by a trusted source (310) connected to the trusted base computer (24).

3. A wireless communication device as in claim 1 wherein said new random data is a combination or permutation of plural random data obtained by the trusted base computer (24) from at least one of the following sources:

   a software random number generator (306);

   a hardware random number generator (308); or

   a remote secure website (310).

4. A wireless communication device as in claim 1 wherein said device further comprises:

   a random data generator configured to accept random number seed input from said random pool database.

5. A wireless communication device as in claim 1 wherein said secure data input port comprises a wired connector suited for wired connection to a user's own trusted computer.

6. A wireless communication device as in claim 1 wherein said secure data input port comprises an encrypted wireless input communications channel.

7. A wireless communication device as in claim 1 wherein said secure data input port comprises:

    a wired connector suited for wired connection to a user's own trusted computer; and

    an encrypted wireless input communications, channel.

8. A method comprising:

    storing random data in a random pool database (300) of a wireless communication device (100) having a secure data input port (118) for receiving random data from a trusted base computer (24); and

    adding randomness to the random pool database by storing added new random data received from the trusted base computer (24) in said random pool database based on new input data securely received via said input port (118) each time the device is connected for data synchronization with the trusted base computer.

9. A method as in claim 8 wherein the added new random data received from the trusted base computer (24) is generated by a trusted source (310) connected to the trusted base computer (24).

10. A method as in claim 8 wherein said new random data is a combination or permutation of plural random data obtained by the trusted base computer (24) from at least one of the following sources:

    a software random number generator (306);

    a hardware random number generator (308); or

    a remote secure website (310).

11. A method as in claim 8 wherein said method further comprises:

accepting random number seed data into a random data generator from said random pool database.

12. A method as in claim 8 wherein said secure data input port provision comprises establishing a wired connection to a user's own trusted computer.

13. A method as in claim 8 wherein said secure data input port comprise establishing encrypted wireless input communications channel.

14. A method as in claim 8 wherein said secure data input port comprises:

establishing a wired connection to a user's own trusted computer; and

establishing an encrypted wireless input communications channel.

15. A computer program medium having stored therein a computer program which, when executed, in a wireless communication device (100) configured to implement cryptographic functions utilizing random data input causes:

storage of new random data in a random pool database (300) of said wireless device based on new data securely received via a secure data input port (118) from a trusted base computer (24), as needed for subsequent device operation; and

adding randomness to the random pool database by storing added new random data in said random data pool database (118), each time the device is connected for data synchronization with the trusted base computer.

16. A computer program medium, as in claim 15, wherein said program, when executed, causes said new random data to replace entirely the random data previously stored in said random pool database.

17. A computer program medium as in claim 15, wherein said new random data is a combination or permutation of plural random data obtained by the trusted base computer (24) from at least one of the following sources:

a software random number generator (306);
a hardware random number generator (308); or
a remote secure website (310).

18. A base system (24) comprising: a secure input/output data port (72) for use with a wireless communication device (100), said base system being **characterized by**:
a control processor (24) configured to provide new random data to be added to a random pool database (300) in said wireless communication device (100) via said secure input/output data port each time the device is securely connected for data synchronisation with the base system.

19. A base system as in claim 18 wherein said secure input/output data port includes a trusted wired connection.

20. A base system as in claim 18, wherein said secure input/output data port includes a cryptographically secured wireless communication link.

21. A base system as in claim 18 wherein said control processor is configured to generate said new random data from a software random number generator (306) accessible to said control processor.

22. A base system as in claim 18 wherein said control processor is configured to generate said new random data from a hardware random number generator (308) accessible to said control processor.

23. A base system as in claim 18 wherein said control processor is configured to fetch new random data from a securely maintained and accessible external network site (310).

24. A base system as in claim 19 wherein said control processor is configured to generate said new random data from a hardware random number generator (308) accessible to said control processor.

25. A base system as in claim 19 wherein said control processor is configured to fetch new random data from a securely maintained and accessible external network site (310).

26. A base system as in claim 18 wherein said control processor is configured to obtain said new random data from at least one of the following sources, if accessible:

    a software random number generator (306);

    a hardware random number generator (308); or

    a remote secure website (310).

27. A base system as in claim 26, wherein said control processor is configured to obtain said new random data using as many of said sources as are then accessible.

28. A base system as in claim 26 wherein said new random data is a combination or permutation of plural random data obtained from plural of said sources.

29. A method for operating a base system (24) with a secure input/output data port for use with a wireless communication device (100) including implementation of cryptographic functions utilizing random input data, said method comprising:

    sending new random data to said wireless communication device via said secure input/output data port (118,102) for addition to a random pool database (300) in said wireless communication device (100) each time the device is connected for data synchronisation with the base system.

30. A method as in claim 29 wherein said secure input/output data port includes a trusted wired connection.

31. A method as in claim 29 wherein said secure input/output data port includes a cryptographically secured wireless communication link.

32. A method as in claim 29 wherein said new random data is generated using a software random number generator (306).

33. A method as in claim 29 wherein said new random data is generated using a hardware random number generator (308).

34. A method as in claim 29 wherein said new random data is generated using a securely maintained and accessible external network site (310).

35. A method as in claim 32 wherein said new random data is generated in conjunction with a hardware random number generator (308).

36. A method as in claim 32 wherein said new random data is generated in conjunction with a securely maintained and accessible external network site (310).

37. A method as in claim 29 wherein said new random data is obtained from at least one of the following sources, if accessible:

a software random number generator (306);
a hardware random number generator (308); or
a remote secure website (310).

38. A method as in claim 37 wherein said new random data is generated using as many of said sources as are then accessible.

39. A method as in claim 38 wherein said new random data is generated by combining or permuting plural random data obtained from plural of said sources.

40. A computer program medium having stored therein a computer program, which when executed, in a base system (24) causes:

new random data to be generated and sent to be added to a random pool database (300) in a wireless communication device (100) each time the wireless communication device is connected for data synchronisation with the base system via a secure input/output port (118).

41. A computer program medium as in claim 40 wherein said new random data is generated using a software random number generator (306).

42. A computer program medium as in claim 40 wherein said new random data is generated using a hardware random number generator (308).

43. A computer program medium as in claim 40 wherein said new random data is fetched from a securely maintained and accessible external network site (310).

44. A computer program medium as in claim 41 wherein said new random data is generated in conjunction with a hardware random number generator (308).

45. A computer program medium as in claim 41 wherein said new random data is generated in conjunction with a securely maintained and accessible external network site (310).

46. A computer program medium as in claim 40 wherein said new ransom data is obtained from at least one of the following sources, if accessible:

a software random number generator (306);
a hardware random number generator (308); or
a remote secure website (310).

47. A computer program medium as in claim 46 wherein said new random data is obtained using as many of said sources as are then accessible.

48. A computer program medium as in claim 47 wherein said new random data is a combination or permutation of plural random data obtained from plural of said sources.

49. A wireless communication system comprising:

a mobile wireless communication device (100) configured to implement cryptographic functions utilizing random data input, said device including:

a random pools database (300) configured to store random data for subsequent device operation;
a secure data input port (118); and

a control processor (106) configured tostore random data for subsequent device operation in said random pool database (300) based on new data securely received via said input port (118,102) from a trusted base sub-system (24), the control processor being configured to add randomness to the random pool database by storing added new random data therein, each time the device is connected for synchronisation with the trusted base sub-system, and the trusted base sub-system (24) for use with said wireless communication device (100), said base sub-system including:

a secure input/output data port; and a control processor configured to provide new random data to said random pool database (300) in said wireless communication device (100) via said secure input/output data port each time the device is connected for data synchronization with said base sub-system.

50. A method for operating a wireless communication system comprising a mobile wireless communication device (100) configured to implement cryptographic functions utilizing random data input, said device having a random pool database (300) having random data stored therein for subsequent device operation and a secure data input port (118); and a base subsystem (24) having a secure input/output data port for use with said wireless communication device, said method comprising:

adding new random data in said random pool database (300) based on new data securely received via said input port each time the device is connected for synchronisation with a trusted base sub-system;

sending new random data to said random pool database in said wireless communication device via said secure input/output data port each time the device is connected for synchronisation to the trusted base sub-system.